(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年5 月4 日 (04.05.2006)

PCT

(10) 国際公開番号
WO 2006/046285 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP2004/015896

(22) 国際出願日: 2004 年10 月27 日 (27.10.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 冨樫 昌孝 (TOGASHI, Masataka) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 宮崎 一哉 (MIYAZAKI, Kazuya) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 大野 次彦 (ONO, Tsugihiko) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

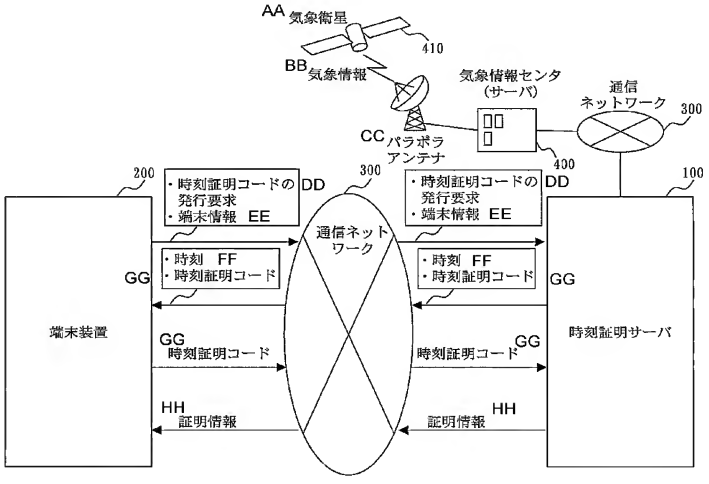
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

[続葉有]

(54) Title: TIME PROOF SERVER, TERMINAL, AND TIME PROVING METHOD

(54) 発明の名称: 時刻証明サーバ、端末装置及び時刻証明方法



AA... METEOROLOGICAL SATELLITE
BB... METEOROLOGICAL INFORMATION
CC... PARABOLA ANTENNA
400... METEOROLOGICAL INFORMATION CENTER (SERVER)
300... COMMUNICATION NETWORK
DD... · TIME PROOF CODE ISSUANCE REQUEST
EE... · TERMINAL INFORMATION
FF... · TIME
GG... · TIME PROOF CODE
HH... · PROOF INFORMATION
200... TERMINAL
100... TIME PROOF SERVER

(57) Abstract: A time proof server comprising a receiving section for receiving a request for issuance of a time proof code and terminal information, a variation-with-time information input section for inputting variation-with-time information, a first code generating section for generating a first code from the variation-with-time information and outputting the first code, a second code generating section for generating a second code form the terminal information and the first code and outputting the second code, a transmitting section for transmitting

[続葉有]

WO 2006/046285 A1

IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

the second code as a time poof code to the terminal, a time proof code storage section for associating the time proof code with the time and storing them, and a proving section for searching the time proof code storage section by using the received time proof code to acquire the time and outputting proof information based on the acquired time to the terminal.

(57) 要約: 時刻証明サーバは、時刻証明コードの発行要求と端末情報とを受信する受信部と、経時変化情報を入力する経時変化情報入力部と、経時変化情報から第１のコードを生成して出力する第１のコード生成部と、端末情報と第１のコードとから第２のコードを生成し出力する第２のコード生成部と、第２のコードを時刻証明コードとして端末装置に送信する送信部と、時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶部と、受信した時刻証明コードにより時刻証明コード記憶部を検索して時刻を取得し、取得した時刻に基づく証明情報を端末装置に出力する証明処理部とを備える。

明 細 書

時刻証明サーバ、端末装置及び時刻証明方法

技術分野

[0001] この発明は、端末装置からの端末情報を時刻と時刻を証明することができる情報と共に記録することにより、端末情報についての時刻の正当性を証明するシステムを構成する時刻証明サーバと端末装置に関する。また、時刻証明サーバと端末装置による時刻証明方法、それをコンピュータで実行する時刻証明プログラムおよび時刻証明プログラムを記録した記録媒体に関する。

背景技術

[0002] 従来、生産物がいつ生産されたのかを明示するために、生産物への生産した年月日や時刻(以降、年月日と時刻とを合わせて「時刻」と表現する)の刻印(表示や印刷を意味する)が行われている。しかし、単に生産物に時刻を刻印するだけでは、それが本当に刻印された時刻に生産されたのかどうかは証明することができない。

[0003] この課題を解決するために特許文献1では、刻印した時刻が正当であることを証明するために、時刻とその時刻で特定される経時変化情報(例えば、その時刻に発表された気象情報など)とを合成して合成情報を生成し、この合成情報を生産物に刻印することにより、後に刻印された合成情報から生産物の生産年月日や時刻を証明することができるシステムと方法とを提案している。

特許文献1:特開2001−297062号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、提案されているシステムと方法は、データの圧縮、位置の測位、データの連結、条件の設定そして経時変化情報の多様化等に関する技術を付加することにより証明の確実性をさらに向上させることが可能である。そこで、この発明は、このような技術を付加することにより、提案されているシステムと方法による証明の確実性をさらに向上させることを目的とする。

課題を解決するための手段

[0005] 時刻証明サーバは、端末装置から、時刻証明コードの発行要求と、端末装置に関する端末情報とを受信する受信部と、経時変化情報を入力する経時変化情報入力部と、経時変化情報入力部が入力した経時変化情報をコード化して第1のコードを生成し、第1のコードを出力する第1のコード生成部と、受信部が受信した端末情報と、第1のコード生成部が出力した第1のコードとに基づいて、第2のコードを生成し出力する第2のコード生成部と、第2のコード生成部が出力した第2のコードを時刻証明コードとして端末装置に送信する送信部と、送信部が送信した時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶部と、端末装置から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶部を検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する証明処理部とを備えたこととした。

[0006] 第1のコード生成部で生成されるコードは完全コードと呼び、気象画像のハッシュ値、端末情報、時刻情報、改ざん検知コードを含んでいる。改ざん検知コードは、気象画像のハッシュ値と端末情報と時刻情報とを連結した値の鍵付きハッシュの値、あるいはディジタル署名の値などである。完全コードのデータサイズは、規定されるものではないが、256バイトから512バイト程度となることが多い。

[0007] 第2のコード生成部で生成されるコードを参照コードと呼び、完全コードのハッシュ値あるいはその一部、端末情報などの付加情報を含んでいる。付加情報には完全コードおよび参照コードのシリアル番号を含んでもよい。参照コードのデータサイズは、12バイトから数十バイトとなる。

[0008] 時刻証明コード記憶部が時刻証明コードを保管するときの情報の対応付けには次のような方法が考えられる。

(1)参照コードと完全コードとを対応付けて保管

(2)端末IDと参照コード、完全コードとを対応付けて保管

(3)参照コードおよび完全コードのシリアル番号と参照コード、完全コードを対応付けて保管

発明の効果

[0009] この発明によれば、時刻を端末装置から受信した端末情報と経時変化情報とを含む情報を圧縮した時刻証明コードに対応させて記憶することにより、後に時刻証明コードにもとづいて時刻を検索し、端末情報についての時刻の正当性を証明する証明情報として公開することができる。

発明を実施するための最良の形態

[0010] 実施の形態1.

第1の実施形態では、証明したい時刻と経時変化情報である気象情報とから合成情報を作成するに際して、ハッシュ関数を用いてデータを圧縮する実施の形態について説明する。

[0011] 図1は、実施の形態1における端末装置と時刻証明サーバとの外観を示す図である。

図1において端末装置と時刻証明サーバとは、システムユニット910、表示装置901、キーボード(K/B)902、マウス903、コンパクトディスク装置(CDD)905、プリンタ装置906、スキャナ装置907を備え、これらはケーブルで接続されている。

[0012] さらに、端末装置と時刻証明サーバとは、FAX機932、電話器931とケーブルで接続され、また、ローカルエリアネットワーク(LAN)942、ウェブサーバ941を介してインターネット940に接続されている。

[0013] 図2は、実施の形態1における端末装置と時刻証明サーバとをコンピュータにより実現した場合のハードウェア構成を示す図である。

図2において端末装置と時刻証明サーバとは、プログラムを実行するCPU(Central Processing Unit)911を備えている。CPU911は、バス912を介してROM(Read Only Memory)913、RAM(Random Access Memory)914、通信ボード915、表示装置901、キーボード(K/B)902、マウス903、FDD(Flexible Disc Drive)904、CDD(Compact Disc Drive)905、プリンタ装置906、スキャナ装置907、磁気ディスク装置920と接続されている。

[0014] RAM914は、揮発性メモリの一例である。ROM913、FDD904、CDD905、磁気ディスク装置920、光ディスク装置は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。

[0015] 通信ボード915は、電話器931、FAX機932、LAN942等に接続されている。通信ボード915、K／B902、FDD904、スキャナ装置907などは受信部や入力部の一例である。また、通信ボード915、表示装置901などは送信部や出力部の一例である。

[0016] ここで、通信ボード915は、LAN942に限らず、直接、インターネット940、或いはISDN等のWAN(Wide Area Network)に接続されていても構わない。直接、インターネット940、或いはISDN等のWANに接続されている場合、端末装置と時刻証明サーバとは、インターネット940、或いはISDN等のWANに接続され、ウェブサーバ941は不用となる。

[0017] 磁気ディスク装置920には、オペレーティングシステム(OS)921、ウィンドウシステム922、プログラム群923、ファイル群924が記憶されている。プログラム群923は、CPU911、OS921、ウィンドウシステム922により実行される。

[0018] プログラム群923には、後述する実施の形態1から実施の形態5の説明において「一部」として説明する機能を実行するプログラムが記憶されている。プログラムは、CPU911により読み出され実行される。

[0019] ファイル群924には、後述する実施の形態1から実施の形態5において、生成した情報やコードや時刻が、ファイルとして記憶されている。

[0020] 後述する実施の形態1から実施の形態5において説明するフローチャートの矢印は主としてデータの入出力を示し、そのデータの入出力のためにデータは、磁気ディスク装置920、FD(Flexible Disc)、光ディスク、CD(Compact Disc)、MD(Mini Disc)、DVD(Digital Versatile Disc)等のその他の記録媒体に記録される。あるいは、信号線やその他の伝送媒体により伝送される。

[0021] 後述する実施の形態1から実施の形態5において「一部」として説明するものは、ROM913に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、ハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。

[0022] 後述する実施の形態1から実施の形態5を実行するプログラムは、また、磁気ディスク装置920、FD(Flexible Disc)、光ディスク、CD(Compact Disc)、MD(Mini

Disc)、DVD(Digital Versatile Disc)等のその他の記録媒体による記録装置を用いて記憶されても構わない。

[0023] 本発明の端末装置と時刻証明サーバとを図1と図2に示すコンピュータシステムで実現する場合について簡単に説明する。まず、図1と図2のコンピュータシステムが起動した状態で、OSが動いているとする。端末装置と時刻証明サーバを実現するプログラムは、磁気ディスク装置920やROM913に格納されている。その実行にあたっては、OSはプログラムを読み取り、RAM914などへの格納するものとする。そうして読み取られたプログラムは逐次実行されていく。これらのコンピュータ上のプログラムの実行については、当業者であれば容易に理解および実施できる事項であるから、本実施の形態の本質部分ではないため、これ以上の詳細な説明には立ち入らない。

[0024] なお、端末装置と時刻証明サーバとをコンピュータにより実現した場合のハードウェア構成は、以降の実施の形態においても、端末装置と時刻証明サーバとを同様に実現できる。

[0025] 図3は、実施の形態1における時刻の証明を実現するシステムの構成を示す図である。

システムは、時刻の証明を依頼する端末装置200と、依頼された時刻の証明を実行する時刻証明サーバ100とそれらを接続する通信ネットワーク300と気象衛星410から受信した気象情報を提供するサーバを備える気象情報センタ400とから構成される。

[0026] 端末装置200は、証明したい端末情報と共に時刻証明コードの発行要求を通信ネットワーク300を介して時刻証明サーバ100へ送信する。端末情報と時刻証明コードの発行要求とを受信した時刻証明サーバ100は、端末装置200に対して端末情報についての時刻を証明する際に必要となる時刻証明コードと時刻を送信する。端末装置200は、時刻証明コードと時刻を受信し、記憶しておく。端末装置200は、後に端末情報の正当性を証明する場合、時刻証明サーバ100へ先に受信した時刻証明コードを送信する。時刻証明コードを受信した時刻証明サーバ100は、商品に刻印する。受信端末その他の端末は、時刻証明コードにもとづいて端末情報の証明情報を生成し、端末装置200へ送信する。端末装置200は、受信した証明情報を用いて

端末情報の正当性を証明する。

[0027] 時刻証明サーバ100の構成を説明する。図4は、時刻証明サーバ100の機能構成を示す図である。

時刻証明サーバ100は、端末装置200から、時刻証明コードの発行要求と、端末装置200に関する端末情報とを受信する受信部101と、経時変化情報を入力する経時変化情報入力部102と、経時変化情報入力部102が入力した経時変化情報をコード化して第1のコードを生成し、第1のコードを出力する第1のコード生成部103と、受信部101が受信した端末情報と、第1のコード生成部103が出力した第1のコードとに基づいて、第2のコードを生成し出力する第2のコード生成部104と、第2のコード生成部104が出力した第2のコードを時刻証明コードとして端末装置200に送信する送信部105と、送信部105が送信した時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶部106と、端末装置200から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶部106を検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置200に出力する証明処理部107とを備える。また、時刻証明サーバ100は、時刻証明コード記憶部106に対して時刻を提供するサーバ電子時計108を備える。

[0028] 時刻証明コード記憶部106が時刻証明コードを記憶する際に情報を対応付ける方法には、

(1)参照コードと完全コードとを対応付けて保管

(2)端末IDと参照コード、完全コードとを対応付けて保管

(3)参照コードおよび完全コードのシリアル番号と参照コード、完全コードを対応付けて保管

がある。

[0029] 受信部101は、端末装置200が通信ネットワーク300を介して送信した端末識別情報(端末ID)を含む端末情報と時刻証明サーバ100に対する時刻証明コードの発行要求を受信し、受信した時刻証明コードの発行要求にしたがって、時刻証明コードの生成を開始し、受信した端末情報を後記する第2のコード生成部104へ送る。

[0030] 端末情報は、証明したい時刻に加えて、端末装置200の端末識別情報(端末ID:I

dentifier）や端末装置200の利用者の識別情報、契約の識別情報などを含んでいる。また、端末情報は、端末装置でしか生成できない情報や、その端末装置と時刻証明サーバでしか生成できない情報、あるいは、暗号により交換できない情報として実現される。

[0031] 時刻証明コードは、受信部101が受信した端末情報と気象衛星410から受信した気象情報とから生成され、生成した時刻証明コードを端末装置200へ送信すると共に、時刻証明コードを時刻に対応させて記憶することにより、後に時刻証明コードを用いて、時刻証明コードに含まれる証明したい情報についての時刻の正当性を証明することが可能となる。

[0032] 経時変化情報入力部102は、気象情報センタ400のサーバから気象情報を含む経時変化情報を入力し、第1のコード生成部103へ送る。

[0033] 第1のコード生成部103は、図5に示すように、経時変化情報入力部102から受け取った気象情報を含む経時変化情報を符号化してディジタル情報、例えば、ビットマップデータを生成し、さらに、ハッシュ関数を用いて生成したビットマップデータの第1段階ハッシュ生成を行い、ハッシュ値を生成して完全コード（第1のコードの一例）を得て、第2のコード生成部104へ送る。ハッシュ関数を用いてビットマップデータのハッシュ値を得ることにより、ビットマップデータは、20バイトから64バイト程度のデータに圧縮される。

[0034] 第2のコード生成部104は、図5に示すように、第1のコード生成部103から受け取った完全コードに、受信部101から受け取った端末識別情報（端末ID）を含む端末情報を加えて、第2段階ハッシュ生成を行い、ハッシュ値を生成して参照コード（第2のコードの一例）得て、時刻証明コードとして送信部105へ送る。

[0035] 前記したように端末情報は、端末装置200の利用者の利用者ID、端末装置200が配置されている位置の情報などを含んでいることから、第2のコード生成部104が生成した第2のコードは、端末装置200固有のコードまたは端末装置の利用者固有のコードとなっている。

第1のコード生成部103と同様に第2のコード生成部104でも、ハッシュ関数を用いて端末情報と第1のコードとのハッシュ値を得ることにより、データは、例えば、20バイ

ト程度のデータに圧縮される。ここでは、圧縮された第2のコードを参照コードとも呼ぶことにする。

[0036] 送信部105は、第2のコード生成部104から受け取った第2のコードを時刻証明コードとして、通信ネットワーク300を介して端末装置200へ送信すると共に、時刻証明コード記憶部106へ送る。

[0037] 時刻証明コード記憶部106は、送信部から受け取った時刻証明コードとサーバ電子時計108が随時出力している時刻とを対応させて記憶している。また、端末装置200の端末情報を対応させて記憶している。

[0038] 時刻証明コード記憶部106が時刻証明コードを記憶する際に情報を対応付ける方法には、

(1)参照コードと完全コードとを対応付けて保管

(2)端末IDと参照コード、完全コードとを対応付けて保管

(3)参照コードおよび完全コードのシリアル番号と参照コード、完全コードを対応付けて保管

がある。

[0039] 次に、端末装置200の構成を説明する。図6は、端末装置200の機能構成を示す図である。

時刻証明サーバ100と通信して時刻証明をする端末装置200は、時刻証明コードの発行要求と、端末装置に関する端末情報とを時刻証明サーバ100に送信する時刻証明コード発行要求部201と、時刻証明サーバ100から時刻証明コードを受信し、時刻証明コードにより証明される時刻と時刻証明コードとをならべて印字する刻印部202と

を備える。また、時刻証明サーバ100から受信した時刻証明コードを記憶する時刻証明コード記憶部203を備える。

[0040] 時刻証明コード発行要求部201は、例えば、図6に示すように、タマゴや何かの製品あるいはICタグに、それらを生産した時刻を表示したり書き込んだりしたい場合、端末装置200の端末情報と共に、表示する時刻を証明するための時刻証明コードの発行要求を時刻証明サーバ100へ送信する。なお、端末情報は、証明したい時刻を

含んでいる。刻印部202は、時刻証明サーバ100から受信した時刻証明コードと時刻とを、例えば、タマゴやICタグや何かの製品に、図7に示すように両者対にして刻印する。時刻証明コード記憶部203は、時刻証明サーバ100から受信した時刻証明コードを一時的に記憶する。

[0041] 端末装置200は、さらに、刻印部202が印字した時刻証明コードを入力して時刻証明サーバ100に送信し、時刻証明を要求することにより、刻印部202が印字した時刻の真偽を問う時刻確認部204を備える。なお、時刻確認部204は、独立して、他の端末装置にあってもよい。

[0042] 時刻確認部204は、例えば、タマゴやICタグや何かの製品に、図7に示すように刻印されている時刻が正しいか確認するために、例えば、キーボードから刻印されている時刻証明コードと刻印されている時刻を入力し、時刻証明コードだけを時刻証明サーバ100へ通信ネットワーク300を介して送信する。時刻確認部204は、それを受けて時刻証明サーバ100が送信した証明情報を時刻確認部204は受信し、先に入力した時刻と証明情報に含まれる時刻とが一致するか否かを確認し、結果を表示する。なお、刻印されている時刻と時刻証明コードとの両方を時刻証明サーバ100へ送信して、サーバにおいて確認した結果を証明情報として受けとってもよい。

[0043] または、時刻確認部204は、キーボードから刻印されている時刻証明コードを入力し、時刻証明コードだけを時刻証明サーバ100へ通信ネットワーク300を介して送信する。それを受けて時刻証明サーバ100が送信した証明情報を時刻確認部204は受信し、証明情報に含まれる時刻を表示するようにしてもよい。この場合には、端末装置200の利用者が、刻印されている時刻と表示された時刻とが一致するか否かを目視により比較して確認することとなる。

[0044] なお、実施の形態1では、一つの端末が時刻証明コード発行要求部201と刻印部202と時刻証明コード記憶部203と時刻確認部204とを備えるものとして説明したが、時刻証明コード発行要求部201と刻印部202と時刻証明コード記憶部203を備える端末装置と、時刻確認部204を備える端末とが異なる端末装置であってもよい。

[0045] 次に、実施の形態1における時刻証明サーバ100と端末装置200による時刻証明方法の動作を説明する。

端末装置と時刻証明サーバとを備えた時刻証明システムの時刻証明方法において、端末装置は、時刻証明コードの発行要求と、端末装置に関する端末情報とを時刻証明サーバに送信し、時刻証明サーバは、端末装置から、時刻証明コードの発行要求と、端末に関する端末情報とを受信し、経時変化情報を提供するソース装置から、経時変化情報を入力し、経時変化情報をコード化して第1のコードを生成し、第1のコードを出力し、端末情報と、第1のコードとに基づいて、第2のコードを生成し、第2のコードを出力し、第2のコードを時刻証明コードとして端末装置に送信し、時刻証明コードを時刻に対応させて時刻証明コード記憶部に記憶し、端末装置は、時刻証明コードを時刻証明サーバに送信して、時刻証明を要求し、時刻証明サーバは、端末装置から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶部を検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する。

[0046] この動作を具体的に説明する。まず、生産者の端末装置200が時刻証明サーバ100から時刻を証明するための時刻証明コード受信し、証明したい時刻と共に生産物等に刻印する動作を図8に示すフローチャートを用いて説明する。

[0047] 端末装置200の時刻証明コード発行要求部201は、時刻を生産物等に刻印するに際して、刻印する時刻が真実であることを証明するために、時刻証明コードの発行要求と共に、端末装置のIDと証明したい時刻とを含む端末情報を、通信ネットワーク300を介して時刻証明サーバ100に送信する(ステップS100)。

[0048] 時刻証明サーバ100の受信部101は、端末装置200から時刻証明コードの発行要求と端末情報とを受信する(ステップS101)。また、時刻証明サーバ100の経時変化情報入力部102は、気象情報センタ400のサーバから気象情報を、随時、入力している(ステップS102)。時刻証明サーバ100の第1のコード生成部103は、端末情報に含まれる証明したい時刻の気象情報からハッシュ関数を用いて第1段階のハッシュを行って完全コードを生成する(ステップS103)。

[0049] 第1のコード生成部103で生成されるコードは完全コードと呼び、気象画像のハッシュ値、端末情報、時刻情報、改ざん検知コードを含んでいる。改ざん検知コードは、気象画像のハッシュ値と端末情報と時刻情報とを連結した値の鍵付きハッシュの値、

あるいはディジタル署名の値などである。完全コードのデータサイズは、規定されるものではないが、256バイトから512バイト程度となることが多い。

[0050] 第2のコード生成部104で生成されるコードを参照コードと呼び、完全コードのハッシュ値あるいはその一部、端末情報などの付加情報を含んでいる。付加情報には完全コードおよび参照コードのシリアル番号を含んでも良い。参照コードのデータサイズは12バイトから数十バイトとなる。

[0051] 時刻証明コード記憶部106が時刻証明コードを保管するときの情報の対応付けには次のような方法が考えられる。

(1)参照コードと完全コードとを対応付けて保管

(2)端末IDと参照コード、完全コードとを対応付けて保管

(3)参照コードおよび完全コードのシリアル番号と参照コード、完全コードを対応付けて保管

[0052] さらに、時刻証明サーバ100の第2のコード生成部104は、完全コードと端末情報とからハッシュ関数を用いて第2段階のハッシュを行って参照コードを生成し(ステップS104)、送信部105は、生成した参照コードを時刻証明コードとして、サーバ電子時計108で生成した時刻と共に端末装置200へ送信する(ステップS105)。その後、時刻証明サーバ100の時刻証明コード記憶部106は、時刻証明コードを時刻証明サーバ100のサーバ電子時計108で生成した時刻に対応させて記憶する(ステップS106)。

[0053] 端末装置200は、時刻証明サーバ100から時刻証明コードと時刻を受信して時刻証明コード記憶部203に記憶し(ステップS107)、刻印部202が時刻証明コードと時刻とを、生産物等に刻印する(ステップS108)。

[0054] 次に、生産物を購入した消費者の端末装置200が、時刻証明サーバ100へ生産物に刻印されている時刻証明コードを送信し、時刻証明サーバ100から時刻証明コードにもとづく時刻を受信することにより、刻印されている時刻の真偽を確認する動作を図9に示すフローチャートを用いて説明する。

[0055] 端末装置200の時刻確認部204は、消費者から生産物に刻印されている時刻証明コードの入力を受け(ステップS110)、時刻証明サーバ100へ通信ネットワーク30

0を介して送信する(ステップS111)。

[0056] 時刻証明サーバ100の証明処理部107は、時刻証明コードを受信し(ステップS112)、受信した時刻証明コードを用いて時刻証明コード記憶部106を検索して、対応する時刻と端末IDとを取得し(ステップS113)、取得した時刻と端末IDとにもとづく証明情報(この場合は時刻を含む)を生成して端末装置200へ送信する(ステップ114)。なお、証明情報に、端末情報を含ませてもよい。

[0057] 端末装置200の時刻確認部204は、証明情報を受信し(ステップS115)、証明情報に含まれている時刻と生産物に刻印されている時刻とを比較して、刻印されている時刻の真偽の結果を出力する。または、証明情報に含まれている時刻を出力し、消費者は出力された時刻と刻印されている時刻とを比較して、刻印されている時刻の真偽を確認する(ステップS116)。証明情報に端末情報が含まれている場合は、その端末情報を用いて、時刻証明コードを生成した端末装置を表示することができる。

[0058] 以上、説明した時刻証明方法は、端末装置から、時刻証明コードの発行要求と、端末に関する端末情報とを受信する受信処理と、経時変化情報を入力する経時変化情報入力処理と、経時変化情報入力処理により入力した経時変化情報をコード化して第1のコードを生成し、第1のコードを出力する第1のコード生成処理と、受信処理により受信した端末情報と、第1のコード生成処理により出力した第1のコードとに基づいて、第2のコードを生成し出力する第2のコード生成処理と、第2のコード生成処理により出力した第2のコードを時刻証明コードとして端末装置に送信する送信処理と、送信処理により送信した時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶処理と、端末装置から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶処理により記憶した時刻証明コードを検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する証明処理とを時刻証明プログラムとして記述することにより、コンピュータに実行させることができる。この時刻証明プログラムは、記録媒体に記録することができる。

[0059] 以上、実施の形態1における時刻証明サーバ100と端末装置200の動作について説明した。次に、実施の形態1による効果について説明する。

[0060] 実施の形態1によれば、気象情報を含む経時変化情報を用いて端末装置が要求する時刻を証明する時刻証明サーバを実現することが可能となる。

[0061] 実施の形態1によれば、多量のデータを含む画像情報である気象情報であっても、ハッシュを行ってデータを圧縮することにより、時刻を証明するための時刻証明コードのデータ量を小さく抑えることができる。また、時刻証明コードが、短い参照コードとなることにより、端末装置の操作が簡便になる。さらに、一方向性関数であるハッシュ関数を用いてハッシュをおこなうことにより、端末識別情報を含む端末情報と気象情報を含む経時変化情報を分離することができない形式で一体化することができる。

[0062] 実施の形態1によれば、時刻証明サーバに時刻の証明を依頼し、時刻証明サーバが発行した証明する時刻と気象情報を含む経時変化情報からなる時刻証明コードとを時刻を証明したい生産物等に刻印する端末装置を実現することができる。

[0063] 実施の形態1によれば、生産物等に刻印されている時刻を証明するために、時刻証明コードを送信して時刻証明サーバへ時刻の証明を依頼し、時刻証明サーバが発行した証明情報を用いて、刻印されている時刻を証明する端末装置を実現することができる。

[0064] 実施の形態1によれば、時刻証明サーバと端末装置とを用いて、端末装置が提示する時刻を時刻証明サーバが証明する時刻証明方法を実現することができる。

[0065] 実施の形態1によれば、時刻証明方法をプログラムで記述することのより、記録媒体に記録し、時刻証明方法をコンピュータに実現させることができる。

[0066] 実施の形態1によれば、端末識別情報を含めて鍵付きハッシュあるいはディジタル署名を添付することにより、例えば、時刻が同じであっても、端末装置や利用者毎に異なる時刻証明コードを生成することができ、時刻証明コードの盗用を防止することができる。

[0067] 実施の形態1によれば、例えば、ICタグに時刻証明コードを書き込む場合、ICタグでは書き込むデータの長さの制約が緩いことから自由度が大きくなり、生成した完全コードにURL(Uniform Resource Locator)、時刻証明コードを刻印する対象の名称、国名、県名、市町村名などを追加して書き込むことができる。また、他のシステムで用いる情報を取り込むことができる。

[0068] 実施の形態1によれば、端末装置は端末識別情報、利用者の識別情報、契約の識別情報などを端末情報に含めて時刻証明サーバに送信することにより、端末装置やその利用者や利用契約の正当性を認証により確認することができる。

[0069] 実施の形態2.

実施の形態2では、端末装置がGPS(Global Positioning System)衛星から測位時刻情報を受信して端末装置の位置を測位し、端末情報に端末測位情報と測位時刻情報とを含めて時刻証明サーバへ送信する実施の形態について説明する。その際、端末装置は、端末測位情報をより信頼できる情報とするために、端末装置の周辺の温度、湿度、気圧などの位置依存情報を端末情報に含めて送信する。

[0070] 図10は、実施の形態2における時刻の証明を実現するシステムの構成を示す図である。

実施の形態2におけるシステムの構成は、実施の形態1におけるシステムの構成に加えて、端末装置が測位を行うための電波を送信するGPS衛星500を備える。また、端末装置200は、端末情報として端末識別情報(端末ID)に加えて、端末測位情報と測位時刻情報を時刻証明サーバ100へ送信する。端末装置200は、時刻証明コードを取得するために、その位置でしか入手できない情報を時刻証明サーバへ送信して、存在する位置を証明する。これにより、時刻証明サーバ100は、時刻と共に端末装置200が存在する位置を証明する時刻証明コードを発行する。

[0071] 図11は、実施の形態2における時刻証明サーバ100の機能構成を示す図である。実施の形態2における時刻証明サーバ100の構成は、実施の形態1における時刻証明サーバ100の構成に加えて、端末情報が含む測位時刻情報とサーバ電子時計が出力した時刻とを時刻証明コード記憶部106に記録する証明時刻記録部109を備える。

[0072] 証明時刻記録部109は、受信部101が端末装置200から受信した端末情報に含まれた測位時刻情報とサーバ電子時計108により計時された時刻とを、時刻証明コード記憶部106に記録する。

[0073] また、時刻証明サーバ100の受信部101は、端末装置200の位置を測位して得られる端末測位情報、具体的には、GPS衛星500により端末装置200の位置を測位し

て得られる端末測位情報と、GPS衛星500の衛星電子時計から得られる測位時刻情報とを含む端末情報を端末装置200から受信する。また、端末測位情報をより信頼できる情報とするために、受信部101は、端末装置200が存在する位置において端末装置200が取得できる位置依存情報を含む端末情報を端末装置から入力する。

[0074] 時刻証明サーバ100の第2のコード生成部104は、端末測位情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成する。また、第2のコード生成部は、位置依存情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成する。

[0075] 位置依存情報とは、端末測位情報をより信頼できる情報とするための補完的な情報であり、端末装置200が存在する位置でしか入手することができない情報である。例えば、その時刻の、かつ、その位置の気温、湿度、気圧などの気候の情報が位置依存情報である。あるいは、端末装置200が携帯電話やPHS（Personal Handy Phone）（登録商標）の基地局を介して時刻証明サーバ100と接続している場合には、基地局の位置情報が位置依存情報である。あるいは、インターネットを介してデータを伝送している場合には、接続するアクセスルータの位置情報が位置依存情報である。あるいは、電話回線を介してデータを伝送している場合には、経由する交換機など、端末装置が存在する位置を特定することができる情報が位置依存情報である。

[0076] また、実施の形態2で時刻証明サーバ100が備えるサーバ電子時計108は、実施の形態1で時刻証明サーバ100が備えるサーバ電子時計108とは異なり、サーバ電子時計108が、GPS衛星500が備える衛星電子時計と同期を取っている。

[0077] 図12は、実施の形態2における端末装置200の機能構成を示す図である。

実施の形態2における端末装置200の構成は、実施の形態1における端末装置200の構成に加えて、GPS衛星500から電波を受信し、端末装置200の位置を測位する測位部205を備える。

[0078] 測位部205は、通常、4機以上のGPS衛星500から受信した電波に含まれる時刻の情報から電波の到達時間を算出し、算出した到達時間から端末装置の位置を測位する。受信した時刻の情報と測位した位置の情報は時刻証明コード発行要求部2

01に送られる。時刻証明コード発行要求部201は、受信した時刻の情報と測位した位置の情報をそれぞれ測位時刻情報と位置測位情報として端末情報に含めて時刻証明サーバ100へ送信する。または、複数のGPS衛星500から受信した電波に含まれる情報をそのまま時刻証明サーバ100に送信してもよい。

[0079] 次に、実施の形態2における時刻証明サーバ100と端末装置200の動作を図13に示すフローチャートを用いて具体的に説明する。

端末装置200の測位部205は、GPS衛星500から電波を受信し、端末装置200の位置を測位する(ステップS200)。端末装置200は、測位して得られる端末測位情報とGPS衛星500から受信した電波に含まれる測位時刻情報と端末識別情報(端末ID)とを含む端末情報を、時刻証明コードの発行要求と供に時刻証明サーバ100へ送信する(ステップS201)。

[0080] 時刻証明サーバ100は、端末測位情報と測位時刻情報とを含む端末情報と時刻証明コードの発行要求を端末装置から受信し(ステップS202)、端末測位情報と測位時刻情報とを含む端末情報と気象情報を含む経時変化情報とをハッシュして第2のコードを生成する(ステップS203)。

[0081] 以降のステップS204からステップS207までの動作は、実施の形態1における動作の説明の用いた図8のステップS105からステップS108まで動作と同じである。

[0082] なお、ステップS203の動作は、図14に示すようにステップS2031からステップS2033までの動作に置き換えることができる。ステップS2031からステップS2033までのそれぞれの動作は、実施の形態1の図8に示すステップS102からステップS104までの動作と同じである。なお、時刻証明コード記憶部106は、サーバ電子時計108と測位時刻情報とをあわせて記憶しておく。この時刻差が少ないほど、証明力が向上する。

[0083] 以上、実施の形態2における時刻証明サーバ100と端末装置200の動作について説明した。次に、実施の形態2による効果について説明する。

[0084] 実施の形態2によれば、端末装置の位置に用いた測位時刻情報と測位して得た端末測位情報とにより、端末の存在する位置と時刻を証明することができる。

[0085] 実施の形態2によれば、端末測位情報に位置依存情報を時刻を証明するための補

完データとして用いることにより、時刻証明及び端末測位情報の信頼性を向上させることができる。また、位置依存情報をもちいて位置に関する情報の種類を増やすことにより、その中から位置に関する情報を選択して利用することができる。

[0086] 実施の形態2によれば、多量のデータを含む画像情報である気象情報であっても、ハッシュを行ってデータを圧縮することにより、時刻を証明するための時刻証明コードのデータ量を小さく抑えることができる。

時刻証明コードが、短い参照コードとなることにより、端末装置の操作が簡便になる。

また、一方向性関数であるハッシュ関数を用いてハッシュをおこなうことにより、端末識別情報を含む端末情報と気象情報を含む経時変化情報を分離することができない形式で一体化することができる。

[0087] 実施の形態2によれば、端末装置の位置の測位と測位時刻情報の取得にGPSシステムを用いることができる。また、時刻証明サーバは、GPS衛星が備える衛星電子時計が出力した測位時刻情報と、衛星電子時計と同期をとっているサーバ電子時計が出力する時刻とを用いることにより、時刻の精度を向上させることができるので、時刻と測位した位置とが正確になり、許容範囲を越えてずれている信頼できない時刻の申告を発見するなどの証明の精度を向上することができる。

[0088] 実施の形態2によれば、端末装置の位置を測位した端末測位情報を端末情報に含めて、端末装置が提示する時刻を時刻証明サーバが証明する時刻証明方法を実現することができる。

[0089] 実施の形態2によれば、GPS衛星が備える衛星電子時計と時刻証明サーバが備えるサーバ電子時計が時刻の同期をとることにより、測位した位置で入手した測位時刻情報と、時刻証明サーバは端末装置から受け取った時刻との誤差を算出することができるようになり、時刻を証明するための時刻証明コードに記載する時刻を明確にすることができ、また、正確な記録を残すことができる。

[0090] 逆に、端末装置が申告するGPS衛星の衛星電子時計が出力した時刻と時刻証明サーバが出力した時刻とに大きなずれがあれば、端末装置が申告する時刻や位置が不正である可能性が大きくなり、仮に、時刻や位置におおきなずれがあれば、時刻

証明コードの発行を停止するなどの対策を講じることができる。

[0091] 実施の形態3.

実施の形態3では、時刻証明サーバが、先に発行した時刻証明コードと新たに発行する時刻証明コードとを関連づけて記憶することにより、時刻証明コードの発行を要求した端末装置を過去の遡ってトレースすることができる実施の形態について説明する。

[0092] 実施に形態3におけるシステムの構成は、実施の形態1におけるシステムの構成と同じである(図3を参照)。また、時刻証明サーバ100と端末装置200の構成も、実施の形態1と同じである(図4と図6を参照)。

[0093] 実施の形態3における時刻証明サーバ100の受信部101は、既に発行した時刻証明コードを含む端末情報を端末装置200から入力する。第2のコード生成部104は、時刻証明コードを含む端末情報と気象情報を含む経時変化情報とに基づいて、完全コード(第2のコードの一例)を生成する。送信部105は、第2のコード生成部104が出力した完全コードを新たな時刻証明コードとして端末装置200に送信する。

[0094] また、時刻証明サーバ100の時刻証明コード記憶部106は、既に発行した時刻証明コードと新たな時刻証明コードとを、トレース可能なように関連づけて記憶する。この処理を図15に示す。

[0095] 証明処理部107は、端末装置200から、時刻証明コードを受信した場合、受信した時刻証明コードと関連付けられた時刻証明コードを時刻証明コード記憶部106から検索して、検索された時刻証明コードから得られる証明情報を端末装置200に出力する。この処理を図16に示す。他の部分の機能は、実施の形態1のおける各部の機能と同じである。

[0096] なお、端末装置200の各部の機能は、実施の形態1のおける端末装置200の各部の機能と同じである。

[0097] 次に、実施の形態3における時刻証明サーバ100と端末装置200の動作を図17に示すフローチャートを用いて説明する。

実施の形態3における時刻証明方法は、端末装置200が、既に発行した時刻証明コードを含む端末情報を時刻証明サーバ100へ送信し、時刻証明サーバ100は、既

に発行した時刻証明コードを含む端末情報を端末装置200から入力し、時刻証明コードを含む端末情報と経時変化情報とに基づいて、第2のコードを生成し、第2のコードを新たな時刻証明コードとして端末装置200に送信する。

[0098] また、時刻証明サーバ100の時刻証明コード記憶部106は、既に発行した時刻証明コードと新たな時刻証明コードとを、トレース可能なように関連づけて記憶し、時刻証明サーバ100は、端末装置200から、時刻証明コードを受信した場合、受信した時刻証明コードと関連付けられた時刻証明コードを時刻証明コード記憶部106から順に検索して、検索された時刻証明コードから得られる証明情報を端末装置200に出力する。

[0099] 動作を具体的に説明する。

端末装置200は、既に発行済みの時刻証明コードを所持しているものとする。端末装置200の時刻証明コード発行要求部201は、時刻証明コードの発行要求と発行済みの時刻証明コードを含む端末情報とを時刻証明サーバ100へ送信する(ステップS300)。なお、その都度、記載はしないが、端末情報は、当然、端末識別情報(端末ID)と時刻を含んでいる。

[0100] 時刻証明サーバ100の受信部101は、発行済みの時刻証明コードを含む端末情報を受信し(ステップS301)、時刻証明コードを含む端末情報と気象情報を含む経時変化情報とにもとづいて完全コード(第2のコードの一例)を生成する(ステップS302)。そして、時刻証明サーバ100の送信部105は、完全コードを新たな時刻証明コードとして端末装置200へ送信する(ステップS303)。その後、時刻証明サーバ100の時刻証明コード記憶部106は、時刻証明コードを時刻証明サーバ100のサーバ電子時計108で生成した時刻に対応させて記憶する(ステップS304)。

[0101] 端末装置200は、新たな時刻証明コードと時刻を受信し(ステップS305)、刻印部202が時刻証明コードと時刻とを、生産物等に刻印する(ステップS306)。

[0102] なお、ステップS302の動作は、図18に示すようにステップS3021からステップS3023までの動作に置き換えることができる。ステップS3021からステップS3023までのそれぞれの動作は、実施の形態1の図8に示すステップS102からステップS104までの動作と同じである。

[0103] 次に、生産物を購入した消費者の端末装置200が、時刻証明サーバ100へ生産物に刻印されている時刻証明コードを送信し、時刻証明サーバ100から時刻証明コードにもとづく時刻を受信することにより、刻印されている時刻の真偽を確認する動作を図19に示すフローチャートを用いて説明する。

[0104] 端末装置200の時刻確認部204は、消費者から生産物に刻印されている時刻証明コードの入力を受け(ステップS400)、時刻証明サーバ100へ通信ネットワーク300を介して送信する(ステップS401)。

[0105] 時刻証明サーバ100の証明処理部107は、時刻証明コードを受信し(ステップS402)、受信した時刻証明コードを用いて時刻証明コード記憶部106を検索して、対応する時刻と端末IDとを取得すると共に、時刻証明コードに関連する時刻証明コードを順次検索し(ステップS403)、検索した時刻証明コードに対応する時刻と端末IDとから、それぞれに対応する証明情報を生成して端末装置200へ送信する(ステップ404)。

[0106] 端末装置200の時刻確認部204は、証明情報を受信し(ステップS405)、それぞれの証明情報に含まれている端末識別情報(端末ID)を用いて、各端末装置にアクセスし、時刻証明コードが経由した履歴をトレースする。または、各端末装置にアクセスして、指示を与える(ステップS406)。

[0107] 以上、実施の形態3における時刻証明サーバ100と端末装置200の動作について説明した。次に、実施の形態3における効果について説明する。

[0108] 実施の形態3によれば、端末装置は、過去に発行された時刻証明コードを含む新たな時刻証明コードを用いることにより、過去に時刻証明コードを発行した端末装置をトレースでき、履歴を知ることができる。

[0109] 実施の形態3によれば、時刻証明コードが経由してきた端末のトレースを時刻証明コードのみを用いて実現することができ、また、どの端末を経由したのかに関する証明を一度の処理で実現することができる。

[0110] 実施の形態3によれば、ICタグなど記憶できるコードの長さの制約が緩いものでは、一つの時刻証明コードを読み取ることにより、含まれている過去の時刻証明コードに関連する情報を全て獲得することができ、計算やデータの取得効率がよくなるだけ

でなく、過去の情報を活用できるようになり、また、経由に関する情報に確実さを増すことができる。

[0111] 実施の形態3によれば、時刻証明コードを継続的にすることにより、事前の工程で何らかのトラブルが発生し、トレーサビリティ上の問題が発生することを、時刻証明サーバが知りえた段階で、以降の工程に通知することができる。

[0112] 実施の形態4.

実施の形態4では、端末装置が送信した端末情報の内容が条件に一致した場合、時刻証明コードにそのことを示す情報を付加する実施の形態について説明する。

[0113] 実施の形態4におけるシステムの構成は、実施の形態1におけるシステムの構成(図3を参照)と同じである。

[0114] 図20は、実施の形態4における時刻証明サーバ100の機能構成を示す図である。

時刻証明サーバ100は、実施の形態1の構成に加えて、さらに、端末情報から得られた情報が所定の条件に合致するか否かを検出する条件チェック部110と、条件チェック部110が、端末情報から得られた情報が所定の条件に合致することを検出した場合に、第2のコード生成部104に対して、端末情報から得られた情報が所定の条件に合致したことを示す特別コードを付加することを指示する特別コード指示部111を備える。

[0115] 時刻証明サーバ100は、さらに、条件チェック部110が、端末情報から得られた情報が所定の条件に合致することを検出した場合に、第2のコード生成部104が第2のコードを生成することを禁止する禁止部112を備える。

[0116] 条件チェック部110は、端末装置200から受信した端末情報に含まれる端末識別情報(端末ID)、利用者の識別情報、契約の識別情報、時刻などが、定められた所定の条件と合致するか否かを検出する。

[0117] 特別コード指示部111は、端末情報から得られた情報が所定の条件に合致したことを示す信号を条件チェック部110から受信し、その結果を時刻証明コードに記載する必要がある場合、第2のコード生成部104に対して、第2のコードへの特別コードの付加を指示する。

[0118] 禁止部112は、端末情報から得られた情報が所定の条件に合致したことを示す信

号を条件チェック部110から受信し、時刻証明コードを生成してはいけない場合、第2のコード生成部104に対して、第2のコードの生成の禁止を指示する。

[0119] 端末装置200の構成は、実施の形態1における端末装置の構成と同じである。

[0120] 次に、実施の形態4における時刻証明サーバ100と端末装置200の動作を図21に示すフローチャートを用いて説明する。

基本的には、実施の形態2の図13で説明した動作と同じであるが、ステップS202を実行した後、以下の処理を行う。

[0121] 受信部101は、受信した端末情報を条件チェック部110へ送る(ステップS2021)。条件チェック部110は、予め設定してある条件と、端末情報に含まれる端末測位情報、測位時刻情報、位置依存情報(気温、気圧、湿度、基地局IDなど)の少なくともいずれかが合致するか否かを判断する(ステップS2022)。判断した結果、参照コード(第2のコードの一例)に特別コードを付加する条件に合致した場合(ステップS2022のYesの場合)、特別コード指示部111は、第2のコード生成部104に対して、生成する第2のコードに特別コードを含めるように指示する。または、判断した結果、第2のコードを生成してはいけない条件に合致した場合(ステップS2022のYesの場合)、禁止部112は、第2のコード生成部104に対して、第2のコードの生成を禁止する(ステップS2023)。これらの処理を行った後、ステップS203の処理へ移る。また、ステップS2022で判断した結果、条件に合致しなかった場合、ステップS2023は行わずに、ステップS203の処理へ移る。

[0122] 実施の形態4によれば、端末情報の内容が条件に反する場合には、時刻証明サーバが生成する時刻証明コードに、条件に反していることを示す情報を含ませることができる。さらには、時刻証明コード自体の発行を禁止し、問題の拡大を食い止めることが可能となる。

[0123] 例えば、家畜が疫病に感染しているおそれがあることが判明した場合、家畜から生産した食肉の流通を停止するために、流通過程のいずれかにおいて、端末情報の中に、その情報を記述し、条件チェック部110が、その情報を検出することにより、時刻証明コードの発行を禁止して、食肉の流通を禁止したり、または、時刻証明コードにそのことを記述することにより、以降の流通に、その情報を食肉と共に流通させるこ

とができる。

[0124] 食品の保存状態を示す情報として、例えば、保存の際、温度が40度を越えていた場合、食べると危険であることを示す時刻証明コードを発行し、温度が20度以下ならば、食べても問題ないことを示す時刻証明コードを発行することができる。さらに、例としては、時刻証明コードで国内と海外を分けたり、色で分けたりすることができる。

[0125] 実施の形態4によれば、端末装置に予め設定されている条件がある場合、時刻証明サーバが、その条件を受信し、条件に対応する特別な時刻証明コードを発行するような仕組みを実現することができる。

[0126] 例えば、端末装置が盗まれるなどして、その位置が移動した場合、位置が移動したことを検知し、以降の時刻証明コードの発行禁止や位置が移動したことを時刻証明コードに記入することができる。

[0127] 実施の形態5.

実施の形態5では、複数の気象情報の中から適切な気象情報を選択して時刻の証明に利用する実施の形態について説明する。

[0128] 図22は、実施の形態5における時刻の証明を実現するシステムの構成を示す図である。実施の形態5のシステムの構成は、実施の形態1のシステムを構成する気象衛星410および気象情報センタ400が複数となったものである。時刻証明サーバ100と端末装置200の構成は、実施の形態1と同じである。図22では、気象情報センタ400ひとつしかないが複数あってもよい。

[0129] 時刻証明サーバ100の経時変化情報入力部102は、気象情報(経時変化情報の一例)を提供する複数の気象情報センタ400(ソース装置の一例)と接続することができ、時刻に応じて複数の気象情報センタ400の中からいずれかの気象情報センタ400を選択して気象情報を入力する。

[0130] また、時刻証明サーバ100の経時変化情報入力部102は、複数の気象情報センタ400の中からいずれかの気象情報センタ400をランダムに選択して気象情報を入力する。あるいは、所定のアルゴリズムに基づいて気象情報センタ400を選択する。あるいは、気象が激しく変化している気象情報センタ400を選択してもよい。

[0131] 実施の形態5では、時刻証明サーバ100が時刻証明コードを発行するに際して、

複数の気象情報センタ400(例えば、日本と米国と欧州の気象情報センタなど)の中から適切な気象情報センタ400を選択し、そこから気象情報の提供を受けて、実施の形態1で説明したハッシュを行う処理を行うことにより、時刻証明コードを生成する。

時刻証明サーバ100と端末装置200の具体的な動作は、実施の形態1の図8と図9に示す動作と同じである。

[0132] 実施の形態5によれば、複数の気象情報の中から選択して利用することができるので、システム運用の信頼性を向上することができる。また、証明に利用する気象情報の入手間隔を短くすることにより気象情報を取得する密度を高くすることができるので、時刻証明の精度と能力を向上することができる。

図面の簡単な説明

[0133] [図1]実施の形態1における端末装置と時刻証明サーバとの外観を示す図である。

[図2]実施の形態1における端末装置と時刻証明サーバとをコンピュータにより実現した場合のハードウェア構成を示す図である。

[図3]実施の形態1における時刻の証明を実現するシステムの構成を示す図である。

[図4]実施の形態1における時刻証明サーバの機能構成を示す図である。

[図5]実施の形態1における完全コード(第1のコード)と参照コード(第2のコード)を生成方法を示す図である。

[図6]実施の形態1における端末装置の機能構成を示す図である。

[図7]実施の形態1における生産物への刻印の例を示す図である。

[図8]実施の形態1における時刻証明サーバと端末装置による時刻証明方法の動作を示すフローチャートである。

[図9]実施の形態1における端末装置が刻印されている時刻の真偽を確認する動作を示すフローチャートである。

[図10]実施の形態2における時刻の証明を実現するシステムの構成を示す図である。

[図11]実施の形態2における時刻証明サーバの構成を示す図である。

[図12]実施の形態2における端末装置の構成を示す図である。

[図13]実施の形態2における時刻証明サーバと端末装置の動作を示すフローチャー

トである。

[図14]実施の形態2における時刻証明サーバと端末装置の詳細な動作を示すフローチャートである。

[図15]実施の形態3における時刻証明サーバの時刻証明コード記憶部が、既に発行した時刻証明コードと新たな時刻証明コードとをトレース可能なように関連づけて記憶する処理を示す図である。

[図16]実施の形態3における時刻証明サーバの証明処理部が、端末装置から受信した時刻証明コードと関連付けられた時刻証明コードを時刻証明コード記憶部から検索して、得られる証明情報を端末装置に出力する処理を示す図である。

[図17]実施の形態3における時刻証明サーバと端末装置の動作を示すフローチャートである。

[図18]実施の形態3における時刻証明サーバと端末装置の詳細な動作を示すフローチャートである。

[図19]実施の形態3における端末装置が、時刻証明サーバへ時刻証明コードを送信し、時刻証明サーバから時刻証明コードにもとづく時刻を受信することにより、刻印されている時刻の真偽を確認する動作を示すフローチャートである。

[図20]実施の形態4における時刻証明サーバの構成を示す図である。

[図21]実施の形態4における時刻証明サーバと端末装置の動作を示すフローチャートである。

[図22]実施の形態5における時刻の証明を実現するシステムの構成を示す図である。

符号の説明

[0134] 100 時刻証明サーバ、101 受信部、102 経時変化情報入力部、103 第1のコード生成部、104 第2のコード生成部、105 送信部、106 時刻証明コード記憶部、107 証明処理部、108 サーバ電子時計、109 証明時刻記録部、110 条件チェック部、111 特別コード指示部、112 禁止部、200 端末装置、201 時刻証明コード発行要求部、202 刻印部、203 時刻証明コード記憶部、204 時刻確認部、205 測位部、300 通信ネットワーク、400 気象情報センタ、410 気象衛星、

500 GPS衛星、901 表示装置、902 キーボード(K／B)、903 マウス、904 FDD、905 CDD、906 プリンタ装置、907 スキャナ装置、911 CPU、912 バス、913 ROM、914 RAM、915 通信ボード、920 磁気ディスク装置、921 OS、922 ウィンドウシステム、923 プログラム群、924 ファイル群、931 電話器、932 FAX機、940 インターネット、941 ウェブサーバ、942 LAN。

請求の範囲

[1] 端末装置から、時刻証明コードの発行要求と、端末装置に関する端末情報とを受信する受信部と、

経時変化情報を入力する経時変化情報入力部と、

経時変化情報入力部が入力した経時変化情報をコード化して第1のコードを生成し、第1のコードを出力する第1のコード生成部と、

受信部が受信した端末情報と、第1のコード生成部が出力した第1のコードとに基づいて、第2のコードを生成し出力する第2のコード生成部と、

第2のコード生成部が出力した第2のコードを時刻証明コードとして端末装置に送信する送信部と、

送信部が送信した時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶部と、

端末装置から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶部を検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する証明処理部と

を備えたことを特徴とする時刻証明サーバ。

[2] 経時変化情報入力部は、気象情報を含む経時変化情報を入力し、

第1のコード生成部は、気象情報を含む経時変化情報をハッシュして第1のコードを生成することを特徴とする請求項1記載の時刻証明サーバ。

[3] 受信部は、端末識別情報を含む端末情報を端末装置から入力し、

第2のコード生成部は、端末識別情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成することを特徴とする請求項1記載の時刻証明サーバ。

[4] 受信部は、端末装置の位置を測位して得られる端末測位情報を含む端末情報を端末装置から入力し、

第2のコード生成部は、端末測位情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成することを特徴とする請求項1記載の時刻証明サーバ。

[5] 受信部は、端末装置が存在する位置において端末装置が取得できる位置依存情報を含む端末情報を端末装置から入力し、

第2のコード生成部は、位置依存情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成することを特徴とする請求項1記載の時刻証明サーバ。

[6] 受信部は、GPS(Global Positioning System)衛星により端末装置の位置を測位して得られる端末測位情報と、GPS衛星の衛星電子時計から得られる測位時刻情報とを含む端末情報を端末装置から入力し、

時刻証明サーバは、さらに、

GPS衛星の衛星電子時計と同期を取ったサーバ電子時計と、

端末情報に含まれた測位時刻情報と、サーバ電子時計により計時された時刻情報とを、時刻証明コード記憶部に記憶する証明時刻記録部と

を備えたこと特徴とする請求項1記載の時刻証明サーバ。

[7] 受信部は、既に発行した時刻証明コードを含む端末情報を端末装置から入力し、

第2のコード生成部は、時刻証明コードを含む端末情報と経時変化情報とに基づいて、第2のコードを生成し、

送信部は、第2のコード生成部が出力した第2のコードを新たな時刻証明コードとして端末装置に送信することを特徴とする請求項1記載の時刻証明サーバ。

[8] 時刻証明コード記憶部は、既に発行した時刻証明コードと新たな時刻証明コードとを、トレース可能なように関連づけて記憶し、

証明処理部は、端末装置から、時刻証明コードを受信した場合、受信した時刻証明コードと関連付けられた時刻証明コードを時刻証明コード記憶部から検索して、検索された時刻証明コードから得られる証明情報を端末装置に出力する

ことを特徴とする請求項7記載の時刻証明サーバ。

[9] 時刻証明サーバは、さらに、

端末情報から得られた情報が所定の条件に合致するか否かを検出する条件チェック部と、

条件チェック部が、端末情報から得られた情報が所定の条件に合致することを検出した場合に、第2のコード生成部に対して、端末情報から得られた情報が所定の条件に合致したことを示す特別コードを付加することを指示する特別コード指示部を備えたことを特徴とする請求項1記載の時刻証明サーバ。

[10] 時刻証明サーバは、さらに、

端末情報から得られた情報が所定の条件に合致するか否かを検出する条件チェック部と、

条件チェック部が、端末情報から得られた情報が所定の条件に合致することを検出した場合に、第2のコード生成部が第2のコードを生成することを禁止する禁止部を備えたことを特徴とする請求項1記載の時刻証明サーバ。

[11] 経時変化情報入力部は、経時変化情報を提供する複数のソース装置と接続することができ、時刻に応じて複数のソース装置の中からいずれかのソース装置を選択して経時変化情報を入力することを特徴とする請求項1記載の時刻証明サーバ。

[12] 経時変化情報入力部は、複数のソース装置の中からいずれかのソース装置をランダムに選択して経時変化情報を入力することを特徴とする請求項11記載の時刻証明サーバ。

[13] 時刻証明サーバと通信して時刻証明をする端末装置において、

時刻証明コードの発行要求と、端末装置に関する端末情報とを時刻証明サーバに送信する時刻証明コード発行要求部と、

時刻証明サーバから時刻証明コードを受信し、時刻証明コードにより証明される時刻と時刻証明コードとをならべて印字する刻印部と

を備えたことを特徴とする端末装置。

[14] 端末装置は、さらに、

刻印部が印字した時刻証明コードを入力して時刻証明サーバに送信し、時刻証明を要求することにより、刻印部が印字した時刻の真偽を問う時刻確認部を備えたことを特徴とする請求項13記載の端末装置。

[15] 端末装置と時刻証明サーバとを備えた時刻証明システムの時刻証明方法において、

端末装置は、

時刻証明コードの発行要求と、端末装置に関する端末情報とを時刻証明サーバに送信し、

時刻証明サーバは、

端末装置から、時刻証明コードの発行要求と、端末に関する端末情報とを受信し、

経時変化情報を提供するソース装置から、経時変化情報を入力し、

経時変化情報をコード化して第1のコードを生成し、第1のコードを出力し、

端末情報と、第1のコードとに基づいて、第2のコードを生成し、第2のコードを出力し、

第2のコードを時刻証明コードとして端末装置に送信し、

時刻証明コードを時刻に対応させて時刻証明コード記憶部に記憶し、

端末装置は、

時刻証明コードを時刻証明サーバに送信して、時刻証明を要求し、

時刻証明サーバは、

端末装置から、時刻証明コードを受信し、

受信した時刻証明コードにより、時刻証明コード記憶部を検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する

ことを特徴とする時刻証明方法。

[16] 端末装置は、端末装置の位置を測位し、測位して得られる端末測位情報を含む端末情報を時刻証明サーバへ送信し、

時刻証明サーバは、端末測位情報を含む端末情報を端末装置から入力し、端末測位情報を含む端末情報と経時変化情報とをハッシュして第2のコードを生成することを特徴とする請求項15記載の時刻証明方法。

[17] 端末装置は、既に発行した時刻証明コードを含む端末情報を時刻証明サーバへ送信し、

時刻証明サーバは、既に発行した時刻証明コードを含む端末情報を端末装置から入力し、時刻証明コードを含む端末情報と経時変化情報とに基づいて、第2のコードを生成し、第2のコードを新たな時刻証明コードとして端末装置に送信することを特徴とする請求項15記載の時刻証明方法。

[18] 時刻証明コード記憶部は、既に発行した時刻証明コードと新たな時刻証明コードとを、トレース可能なように関連づけて記憶し、

時刻証明サーバは、

端末装置から、時刻証明コードを受信した場合、受信した時刻証明コードと関連付けられた時刻証明コードを時刻証明コード記憶部から順に検索して、検索された時刻証明コードから得られる証明情報を端末装置に出力する

ことを特徴とする請求項17記載の時刻証明方法。

[19] 経時変化情報を提供するソース装置は、複数存在し、

時刻証明サーバは、複数のソース装置と接続することができ、時刻に応じて複数のソース装置の中からいずれかのソース装置を選択して経時変化情報を入力することを特徴とする請求項15記載の時刻証明方法。

[20] 端末装置から、時刻証明コードの発行要求と、端末に関する端末情報とを受信する受信処理と、

経時変化情報を入力する経時変化情報入力処理と、

経時変化情報入力処理により入力した経時変化情報をコード化して第1のコードを生成し、第1のコードを出力する第1のコード生成処理と、

受信処理により受信した端末情報と、第1のコード生成処理により出力した第1のコードとに基づいて、第2のコードを生成し出力する第2のコード生成処理と、

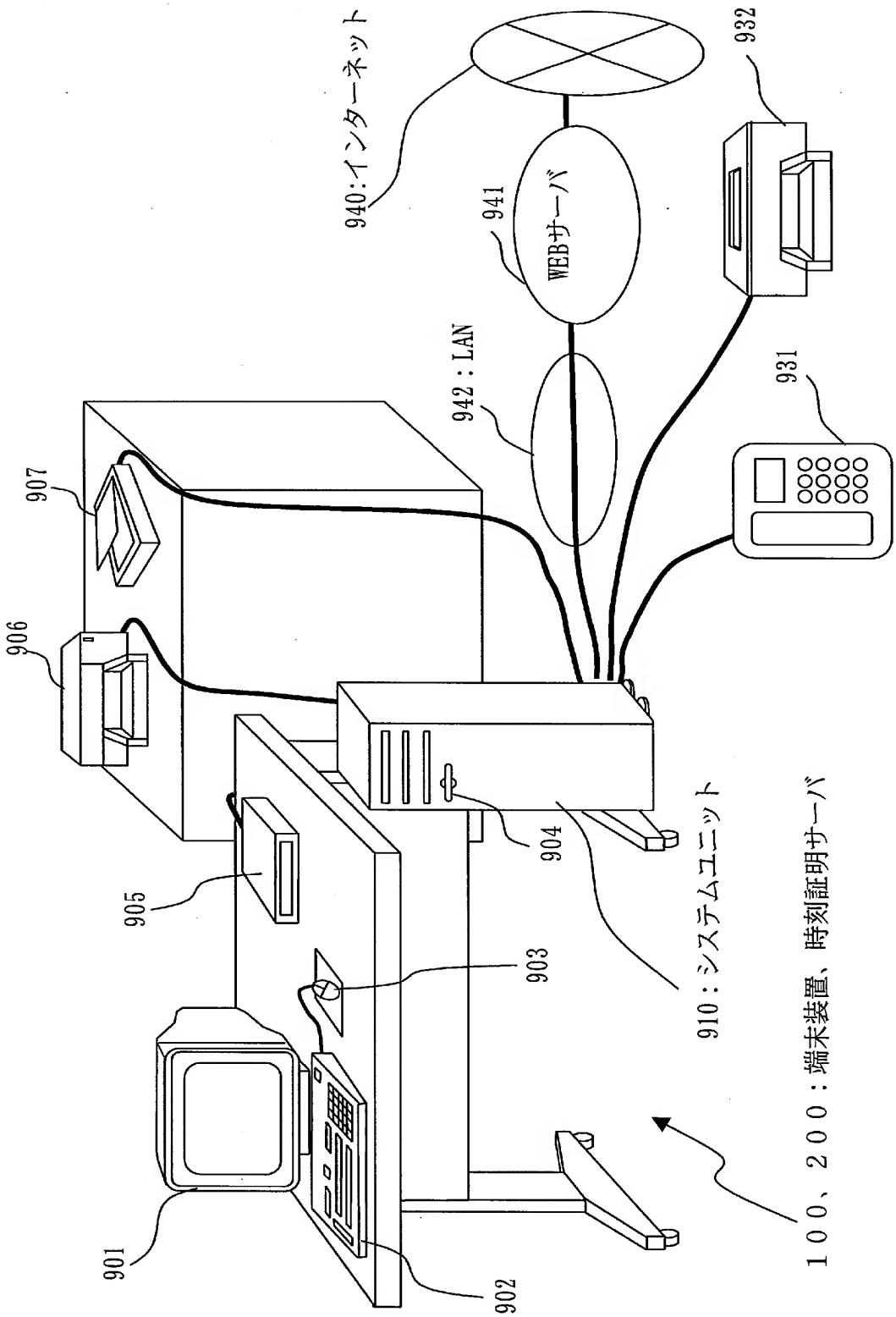
第2のコード生成処理により出力した第2のコードを時刻証明コードとして端末装置に送信する送信処理と、

送信処理により送信した時刻証明コードを時刻に対応させて記憶する時刻証明コード記憶処理と、

端末装置から、時刻証明コードを受信し、受信した時刻証明コードにより、時刻証明コード記憶処理により記憶した時刻証明コードを検索して、時刻証明コードに対応する時刻を取得して、取得した時刻に基づく証明情報を端末装置に出力する証明処理とを

コンピュータに実行させることを特徴とする時刻証明プログラム又はその時刻証明プログラムを記録した記録媒体。

[図1]


940:インターネット
941
WEBサーバ
932
942：LAN
931
907
906
905
904
903
910：システムユニット
901
902
１００、２００：端末装置、時刻証明サーバ

[図2]

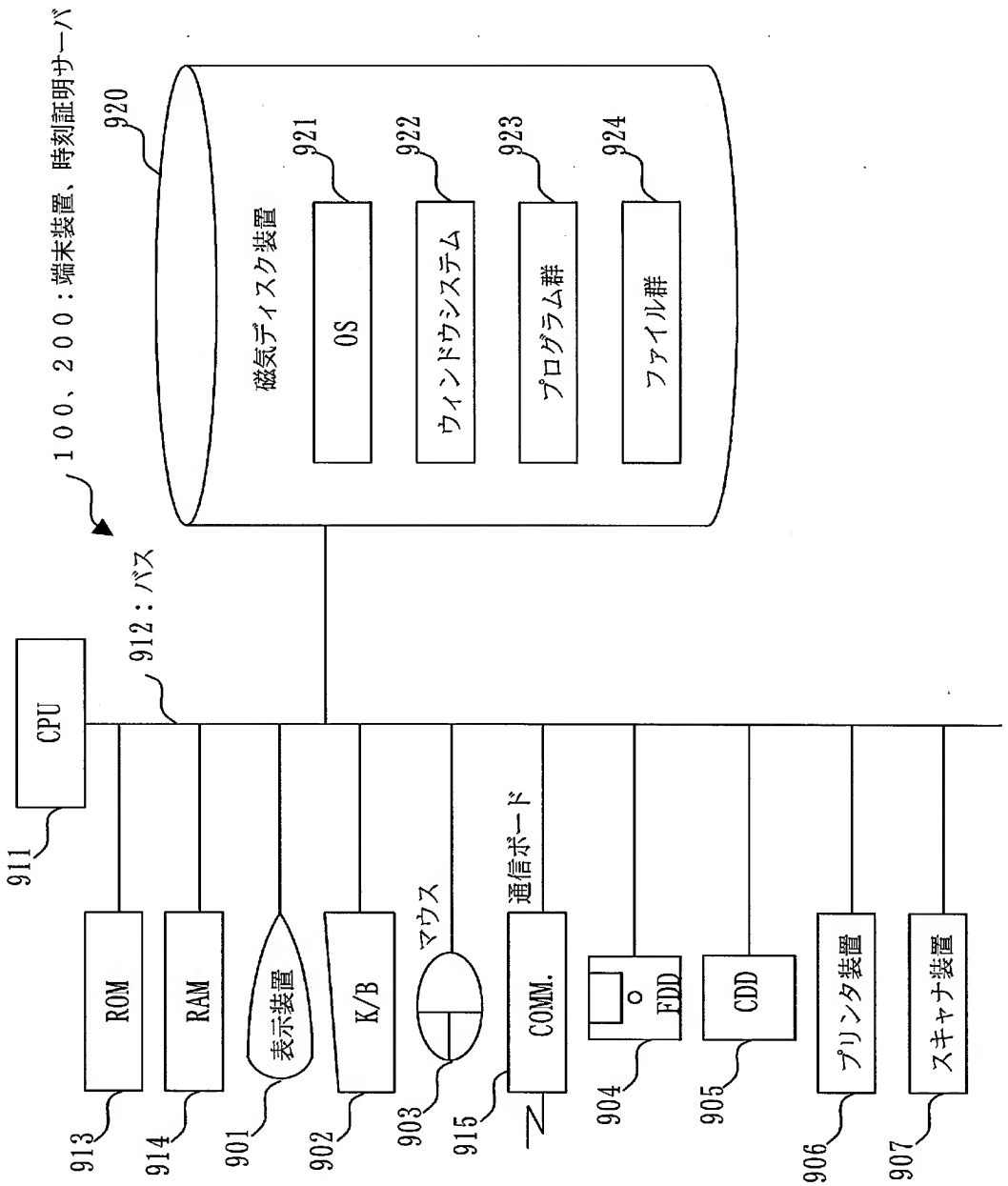

１００、２００：端末装置、時刻証明サーバ
920
磁気ディスク装置
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
912：バス
CPU
911
ROM
913
RAM
914
表示装置
901
K/B
902
マウス
903
通信ボード
COMM.
915
FDD
904
CDD
905
プリンタ装置
906
スキャナ装置
907

図 3

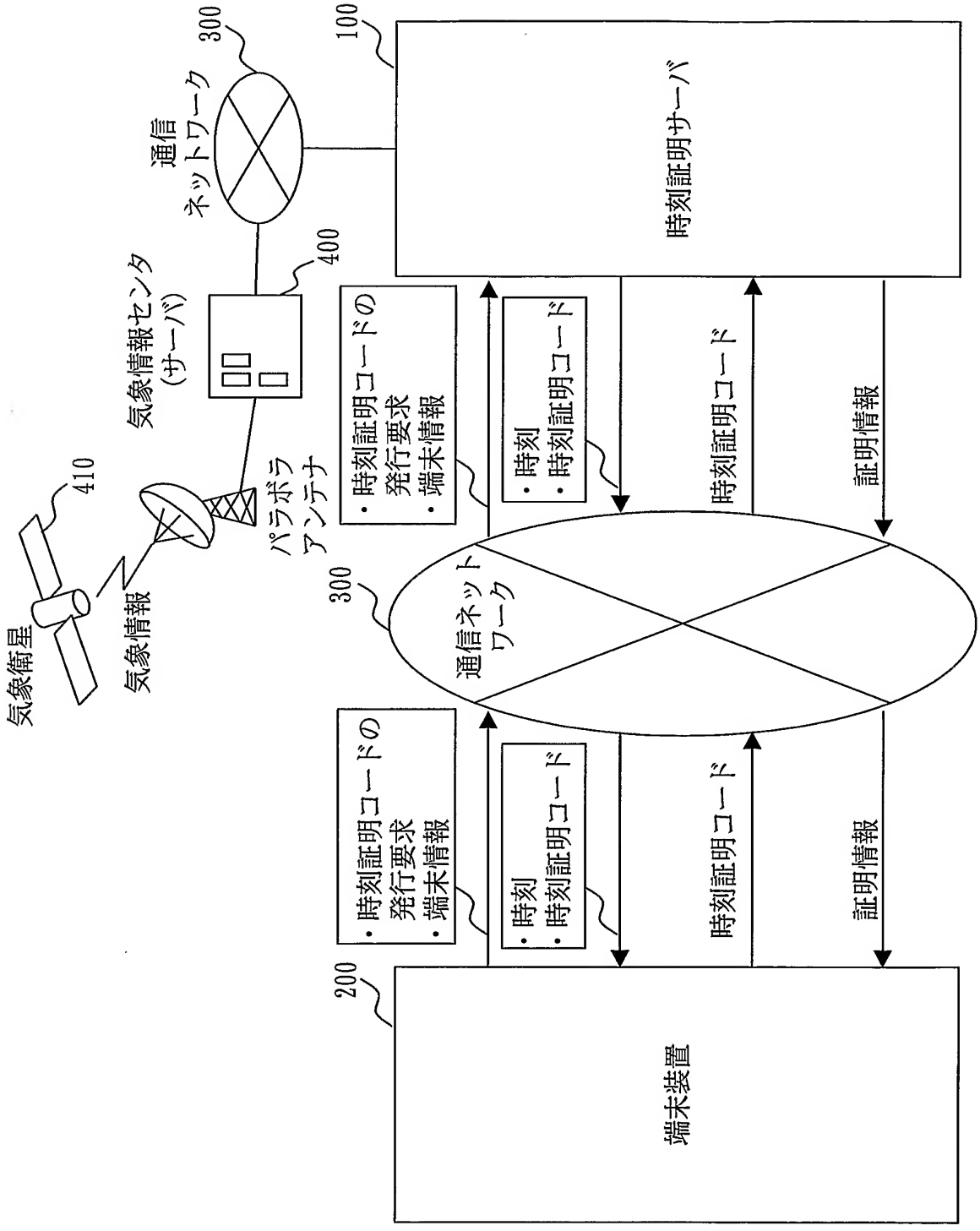

100
時刻証明サーバ
300
通信ネットワーク
400
気象情報センタ(サーバ)
410
気象衛星
気象情報
パラボラアンテナ
・時刻証明コードの発行要求
・端末情報
・時刻
・時刻証明コード
時刻証明コード
証明情報
200
端末装置

図 4

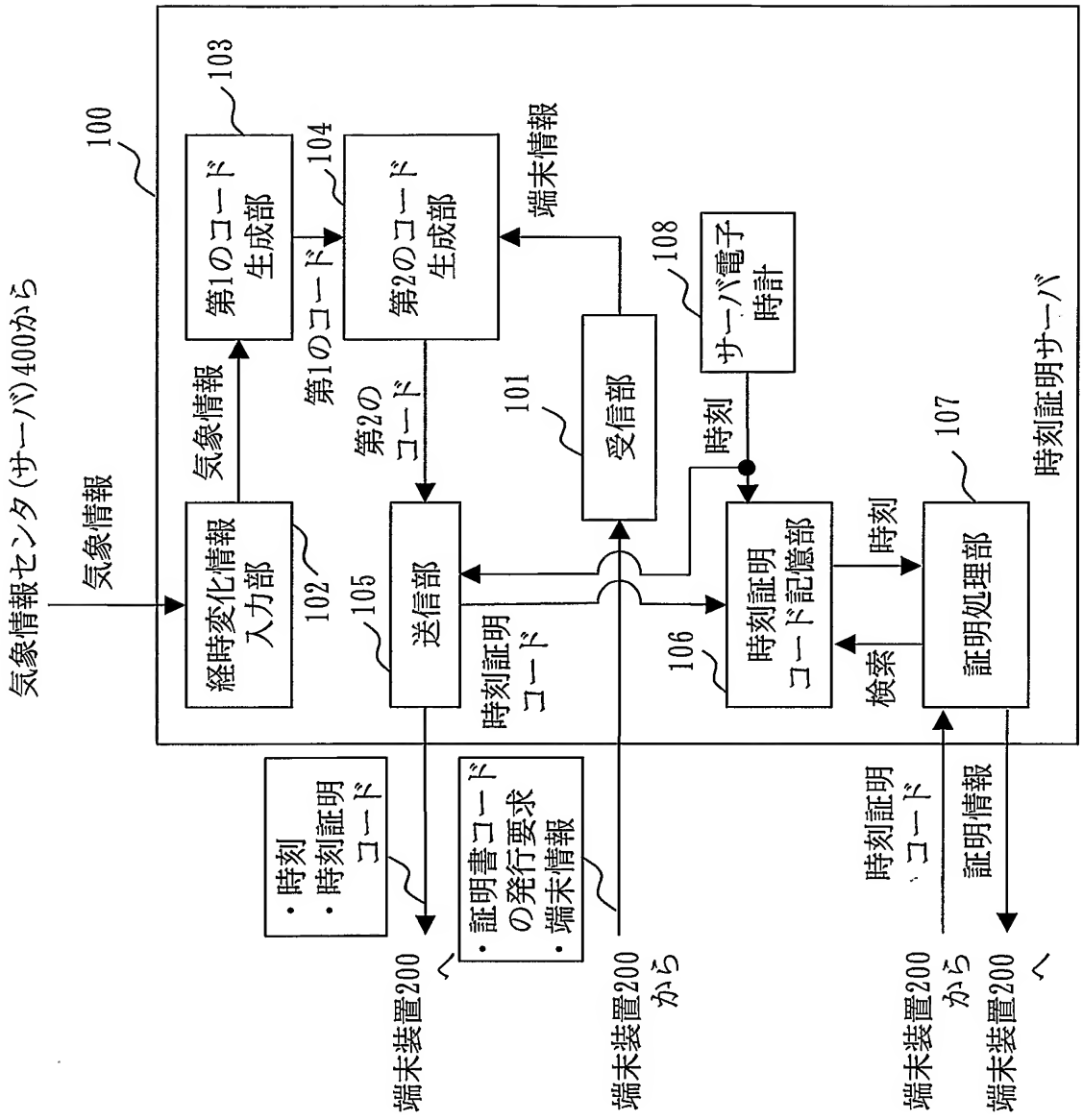

気象情報センタ(サーバ)400から
気象情報
100
経時変化情報入力部
102
気象情報
第1のコード生成部
103
第1のコード
104
第2のコード生成部
第2のコード
端末情報
受信部
101
サーバ電子時計
108
時刻
送信部
105
時刻証明コード
時刻証明コード記憶部
106
検索
時刻
証明処理部
107
時刻証明サーバ
・時刻
・時刻証明コード
・証明書コードの発行要求
・端末情報
時刻証明コード
証明情報
端末装置200へ
端末装置200から
端末装置200から
端末装置200へ

図 5

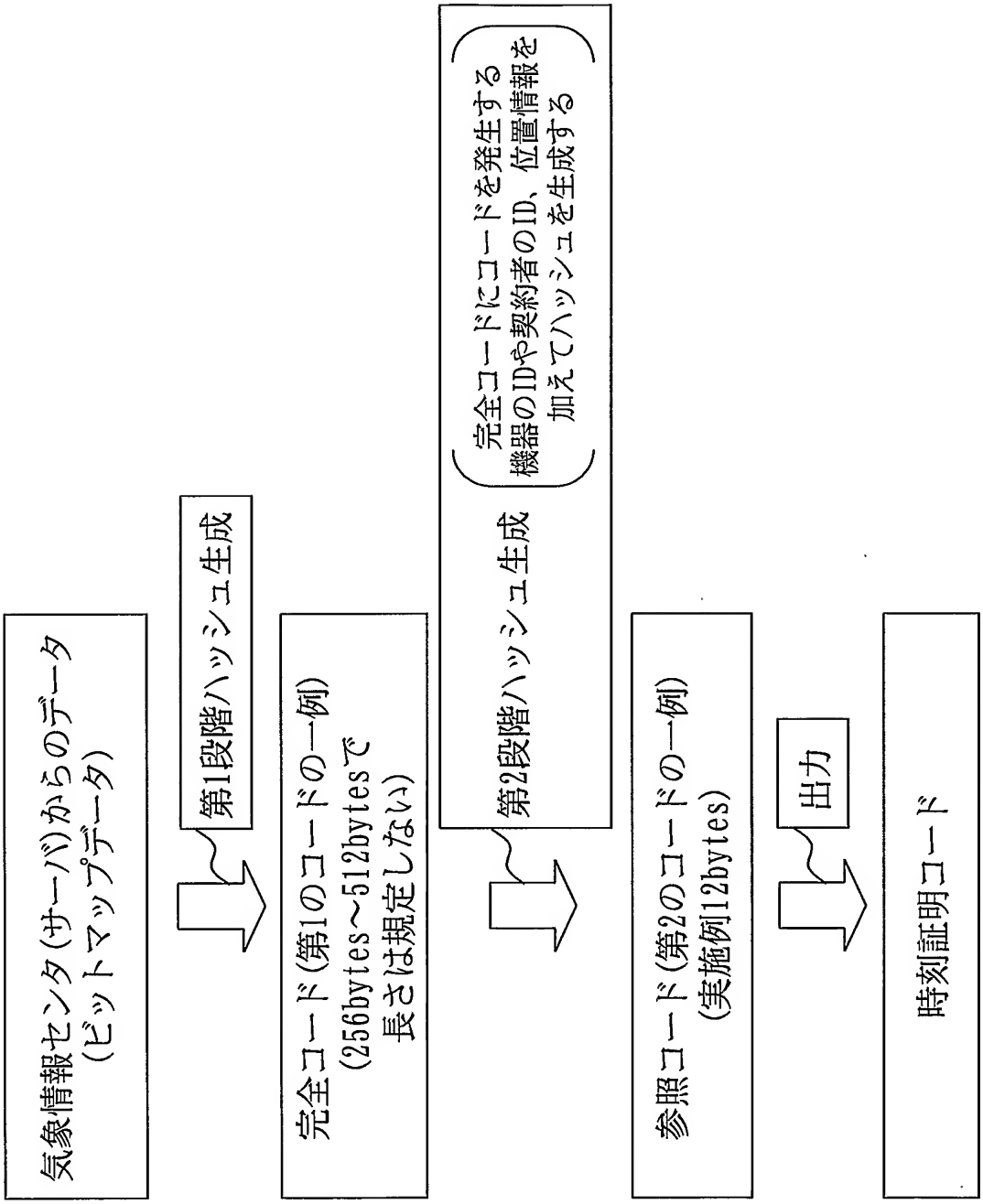
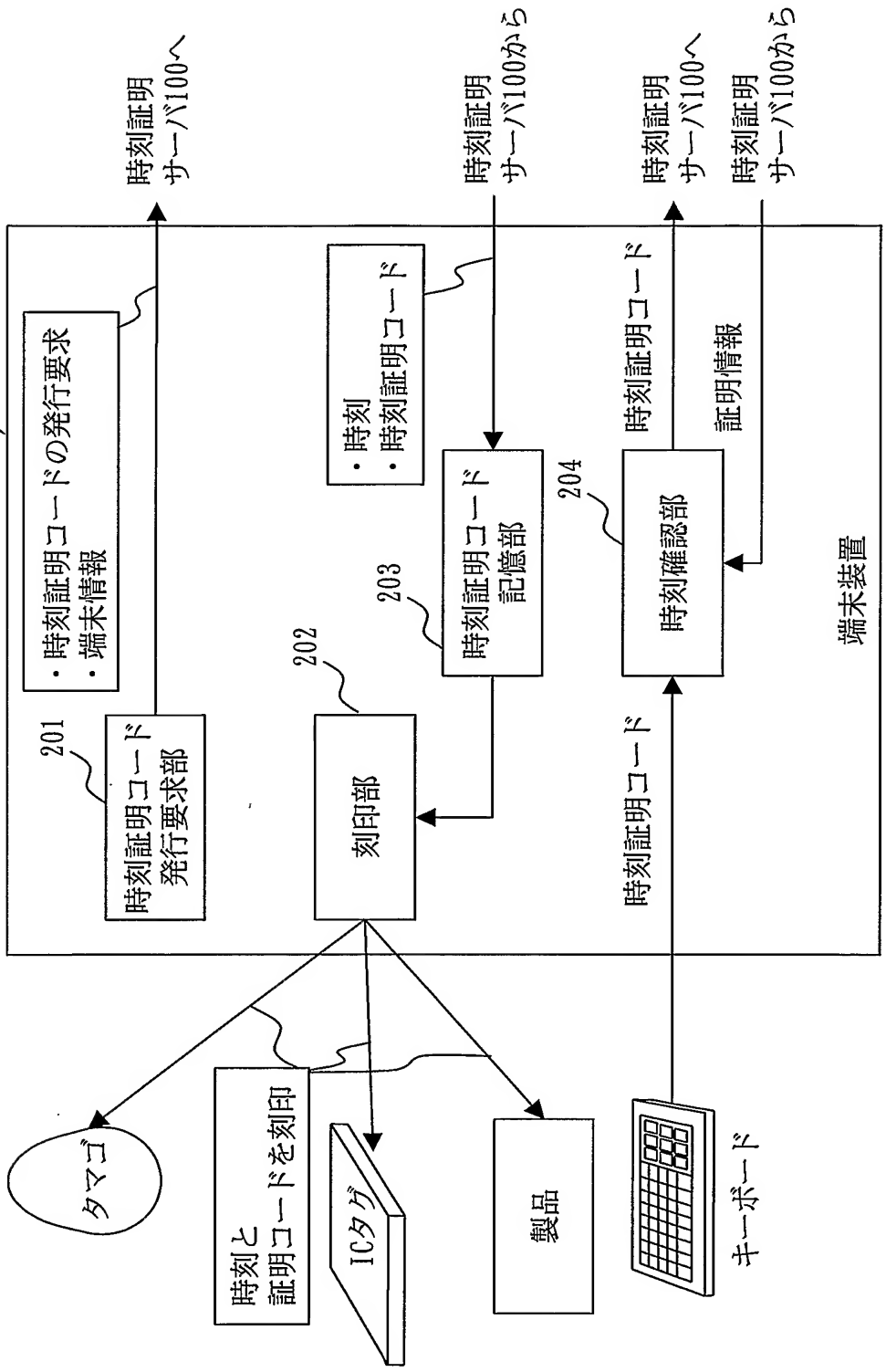
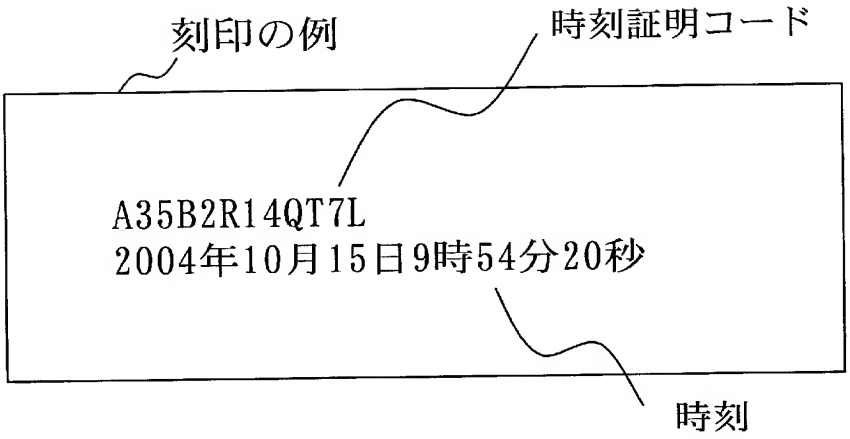

気象情報センタ(サーバ)からのデータ
(ビットマップデータ)
第1段階ハッシュ生成
完全コード(第1のコードの一例)
(256bytes～512bytesで
長さは規定しない)
第2段階ハッシュ生成
(完全コードにコードを発生する
機器のIDや契約者のID、位置情報を
加えてハッシュを生成する)
参照コード(第2のコードの一例)
(実施例12bytes)
出力
時刻証明コード

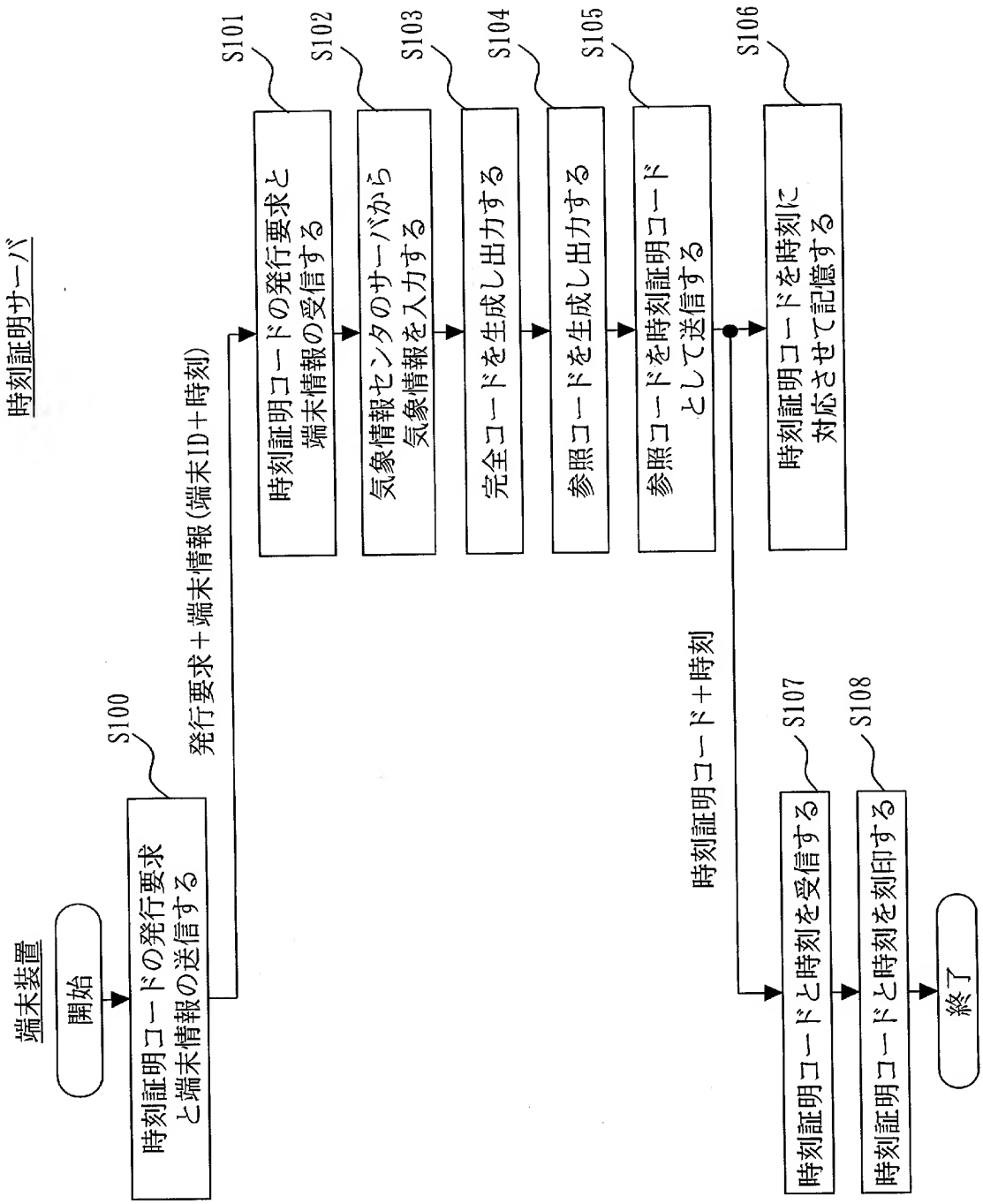
図 6


時刻証明
サーバ100へ
時刻証明
サーバ100から
時刻証明
サーバ100へ
時刻証明
サーバ100から
200
・時刻証明コードの発行要求
・端末情報
・時刻
・時刻証明コード
時刻証明コード
証明情報
204
203
202
201
時刻証明コード
発行要求部
刻印部
時刻証明コード
記憶部
時刻確認部
端末装置
時刻証明コード
タマゴ
時刻と
証明コードを刻印
ICタグ
製品
キーボード

[図7]



[図8]


端末装置
時刻証明サーバ
開始
S100
時刻証明コードの発行要求と端末情報の送信する
発行要求＋端末情報（端末ID＋時刻）
S101
時刻証明コードの発行要求と端末情報の受信する
S102
気象情報センタのサーバから気象情報を入力する
S103
完全コードを生成し出力する
S104
参照コードを生成し出力する
S105
参照コードを時刻証明コードとして送信する
S106
時刻証明コードを時刻に対応させて記憶する
時刻証明コード＋時刻
S107
時刻証明コードと時刻を受信する
S108
時刻証明コードと時刻を刻印する
終了

[図9]

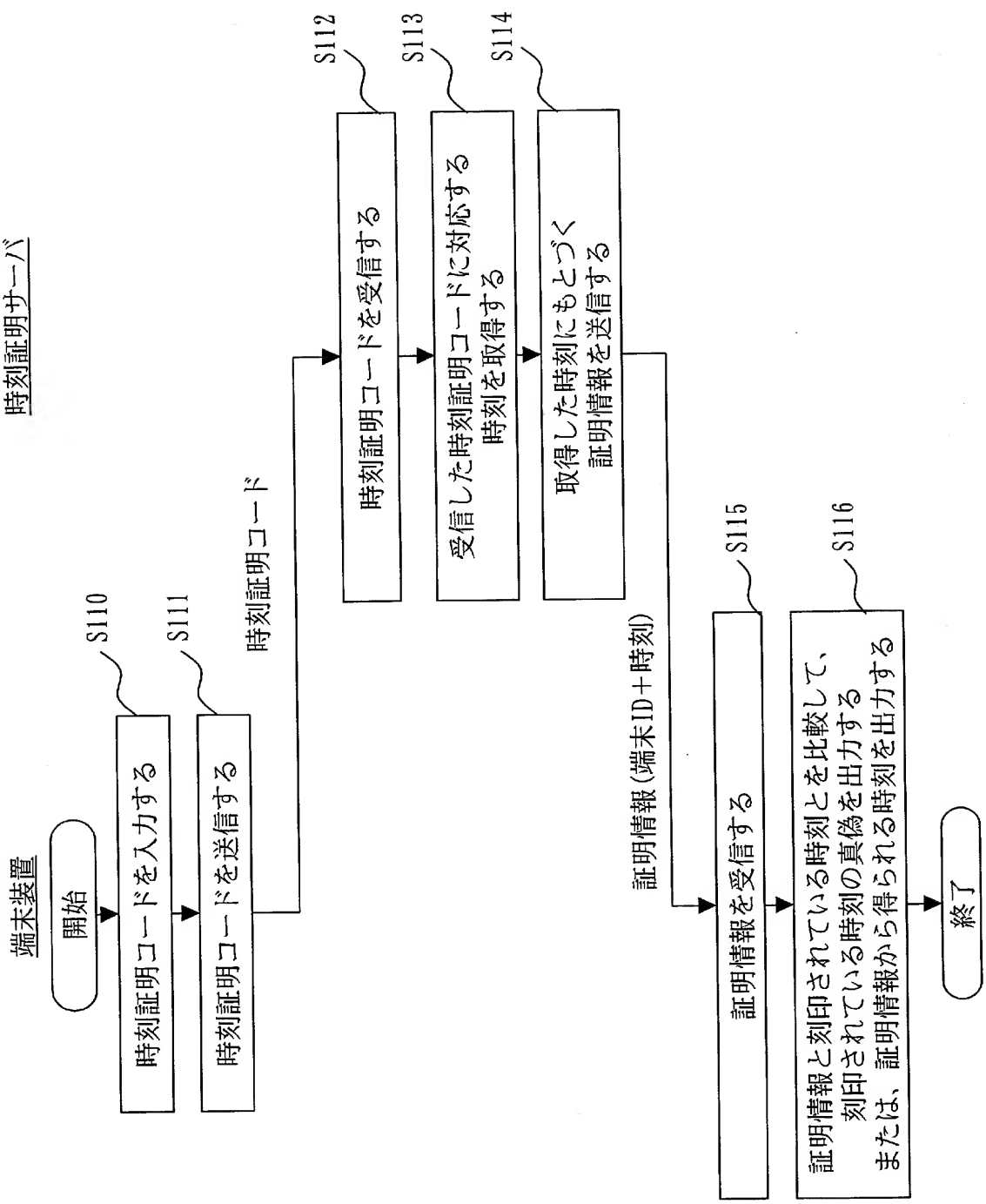

端末装置
時刻証明サーバ
開始
S110
時刻証明コードを入力する
S111
時刻証明コードを送信する
時刻証明コード
S112
時刻証明コードを受信する
S113
受信した時刻証明コードに対応する
時刻を取得する
S114
取得した時刻にもとづく
証明情報を送信する
証明情報（端末ID＋時刻）
S115
証明情報を受信する
S116
証明情報と刻印されている時刻とを比較して、
刻印されている時刻の真偽を出力する
または、証明情報から得られる時刻を出力する
終了

図 10

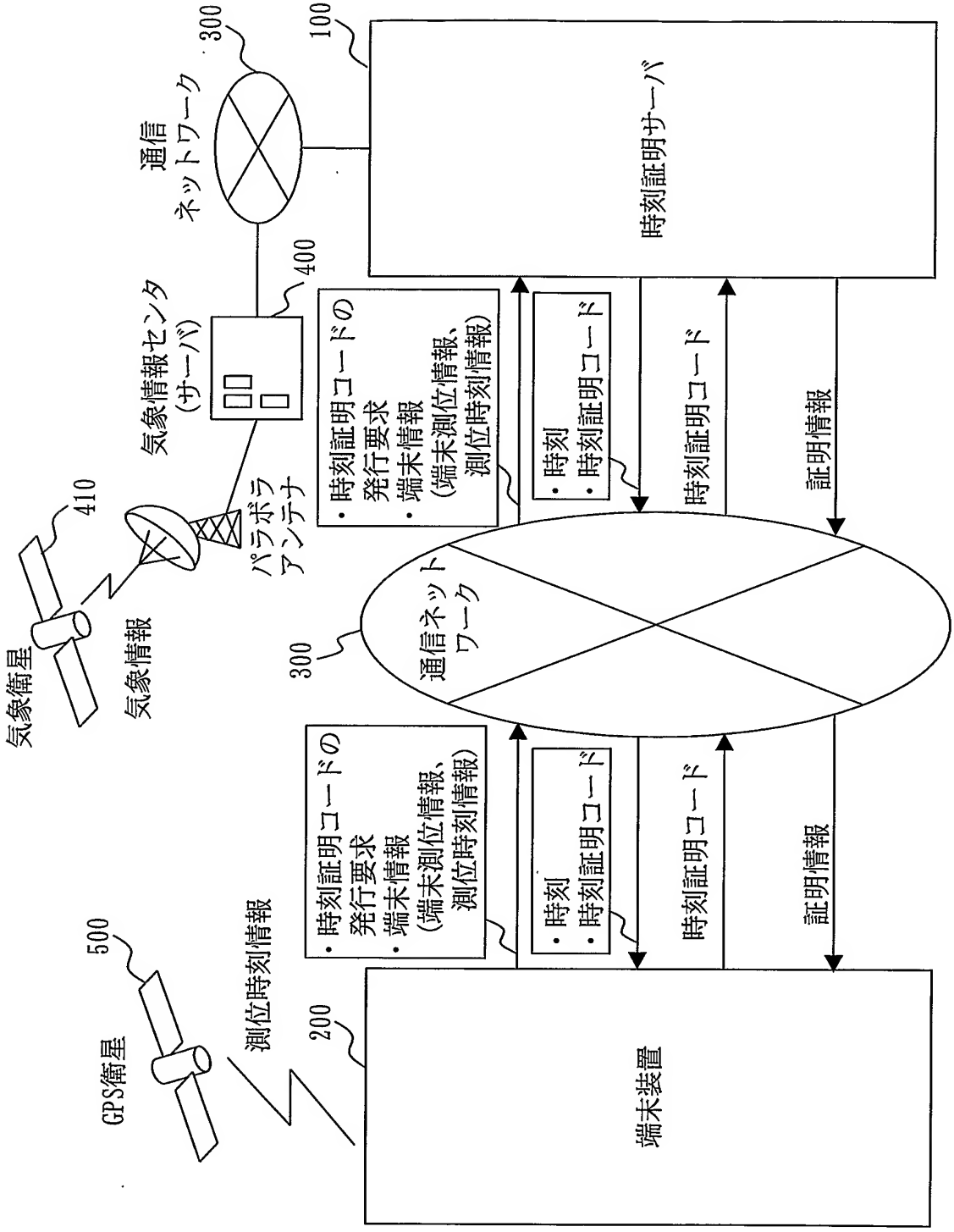

100
時刻証明サーバ
300
通信
ネットワーク
400
気象情報センタ
(サーバ)
パラボラ
アンテナ
410
気象衛星
気象情報
300
通信ネット
ワーク
・時刻証明コードの
発行要求
・端末情報
(端末測位情報、
測位時刻情報)
・時刻
・時刻証明コード
時刻証明コード
証明情報
500
GPS衛星
測位時刻情報
200
端末装置

図 11

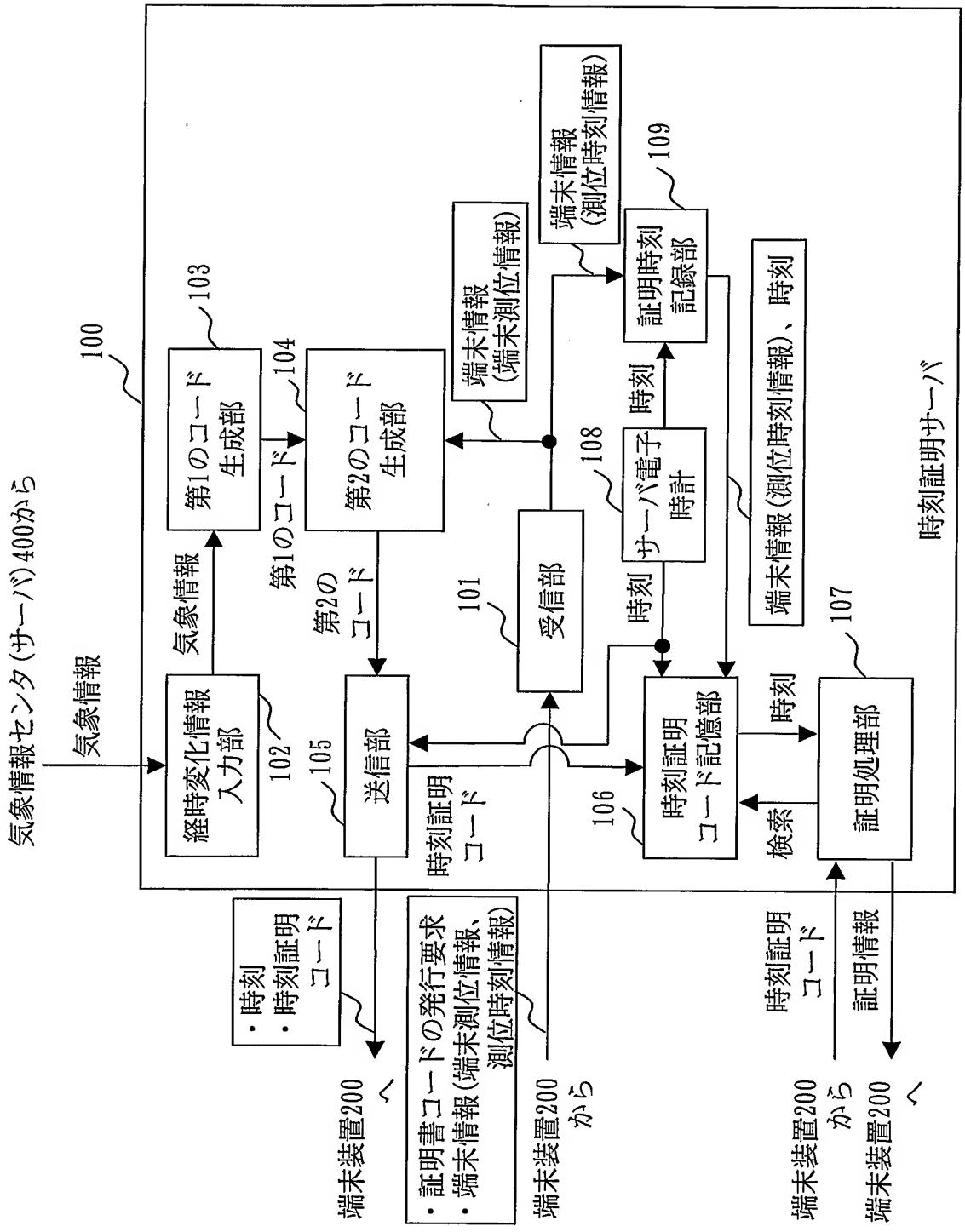
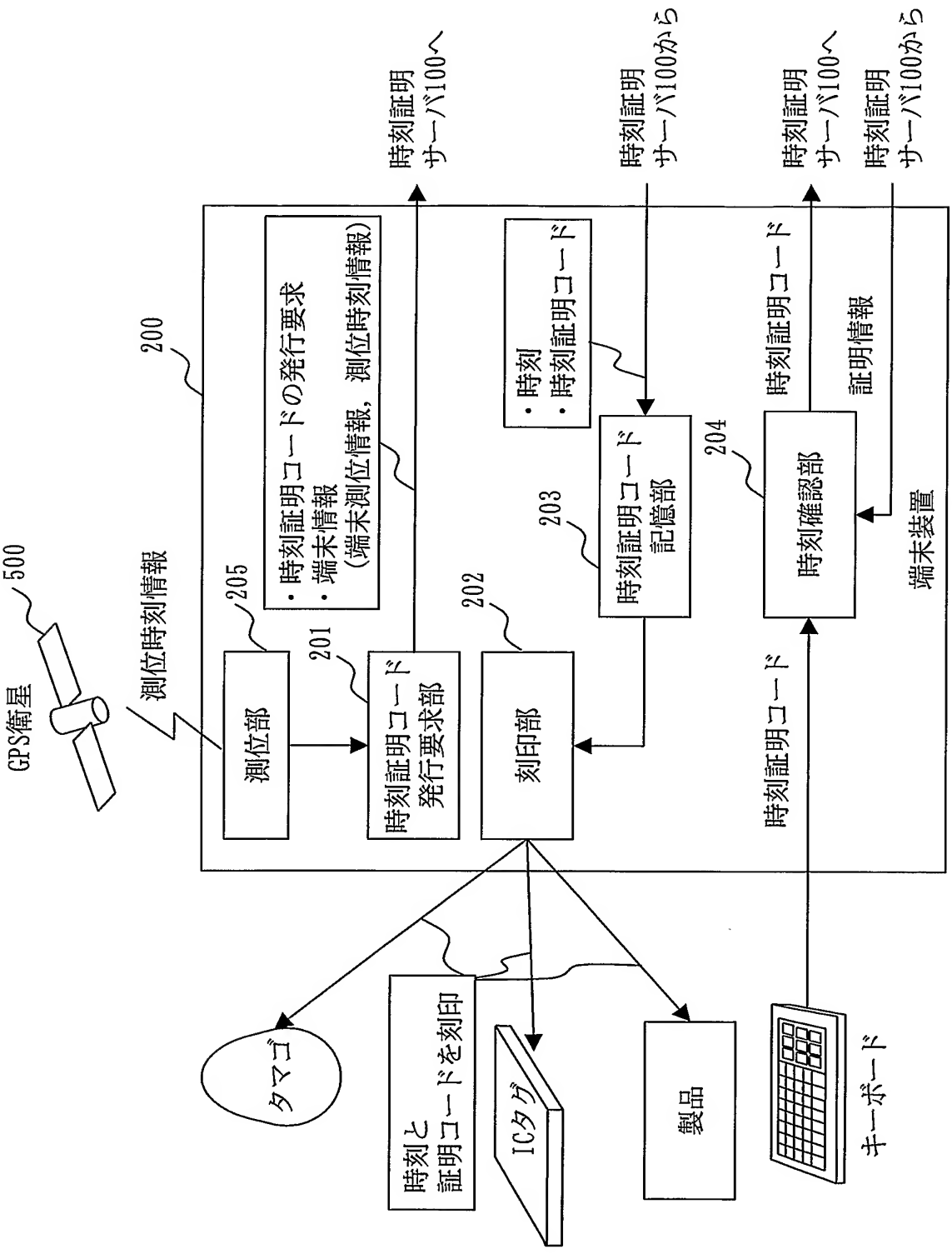

気象情報センタ(サーバ)400から
気象情報
100
経時変化情報入力部
102
気象情報
第1のコード生成部
103
第1のコード
104
第2のコード生成部
第2のコード
105
送信部
時刻証明コード
・時刻
・時刻証明コード
端末装置200へ
・証明書コードの発行要求
・端末情報(端末測位情報、測位時刻情報)
端末装置200から
端末情報(端末測位情報)
受信部
101
端末情報(測位時刻情報)
サーバ電子時計
108
時刻
時刻証明コード記憶部
106
検索
時刻
証明処理部
107
時刻証明コード
証明情報
端末装置200から
端末装置200へ
時刻
証明時刻記録部
109
端末情報(測位時刻情報)、時刻
時刻証明サーバ

図 12



差替え用紙 (規則26)

図 13

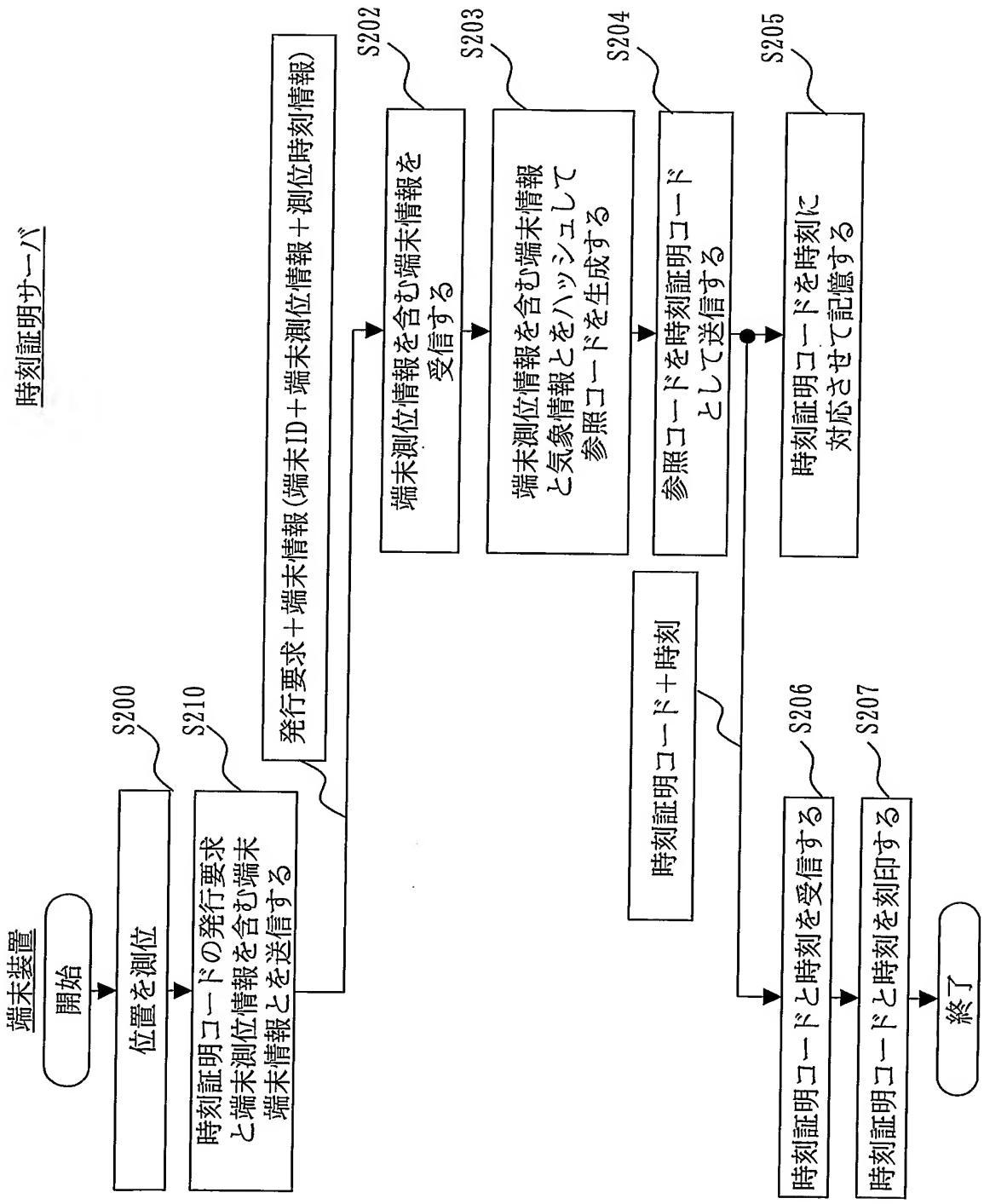

端末装置
時刻証明サーバ
開始
S200
位置を測位
S210
時刻証明コードの発行要求と端末測位情報を含む端末端末情報とを送信する
発行要求＋端末情報（端末ID＋端末測位情報＋測位時刻情報）
S202
端末測位情報を含む端末情報を受信する
S203
端末測位情報を含む端末情報と気象情報とをハッシュして参照コードを生成する
S204
参照コードを時刻証明コードとして送信する
S205
時刻証明コードを時刻に対応させて記憶する
時刻証明コード＋時刻
S206
時刻証明コードと時刻を受信する
S207
時刻証明コードと時刻を刻印する
終了

図 14

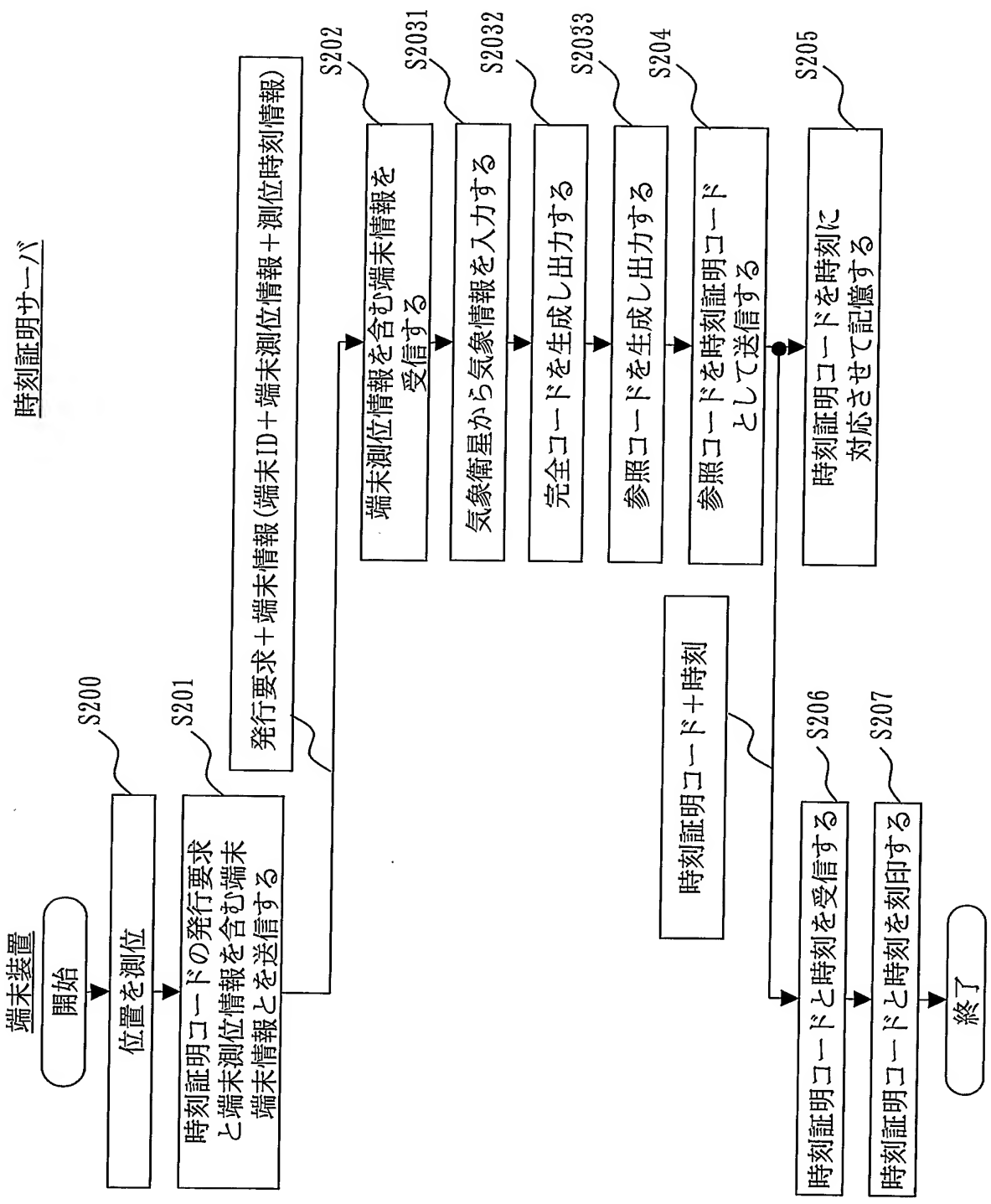
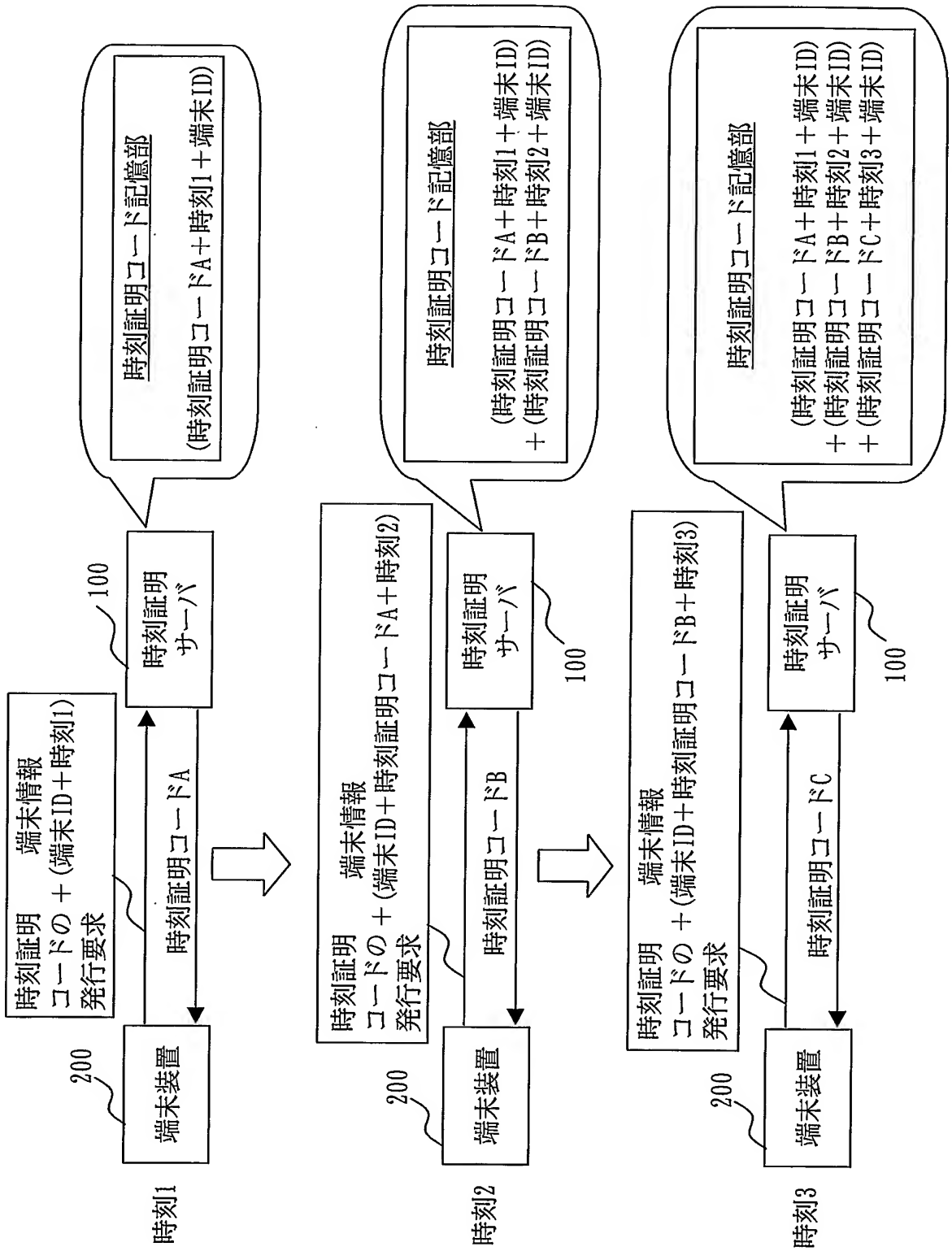

端末装置
時刻証明サーバ
開始
S200
位置を測位
S201
時刻証明コードの発行要求と端末測位情報を含む端末情報とを送信する
発行要求＋端末情報（端末ID＋端末測位情報＋測位時刻情報）
S202
端末測位情報を含む端末情報を受信する
S2031
気象衛星から気象情報を入力する
S2032
完全コードを生成し出力する
S2033
参照コードを生成し出力する
S204
参照コードを時刻証明コードとして送信する
S205
時刻証明コードを時刻に対応させて記憶する
時刻証明コード＋時刻
時刻証明コードと時刻を受信する
S206
時刻証明コードと時刻を刻印する
S207
終了

図 15


時刻証明コード記憶部
(時刻証明コードA+時刻1+端末ID)
時刻証明コードの発行要求
端末情報
(端末ID+時刻1)
時刻証明コードA
時刻証明サーバ
100
端末装置
200
時刻1
時刻証明コード記憶部
(時刻証明コードA+時刻1+端末ID)
+(時刻証明コードB+時刻2+端末ID)
時刻証明コードの発行要求
端末情報
(端末ID+時刻証明コードA+時刻2)
時刻証明コードB
時刻証明サーバ
100
端末装置
200
時刻2
時刻証明コード記憶部
(時刻証明コードA+時刻1+端末ID)
+(時刻証明コードB+時刻2+端末ID)
+(時刻証明コードC+時刻3+端末ID)
時刻証明コードの発行要求
端末情報
(端末ID+時刻証明コードB+時刻3)
時刻証明コードC
時刻証明サーバ
100
端末装置
200
時刻3

[図16]

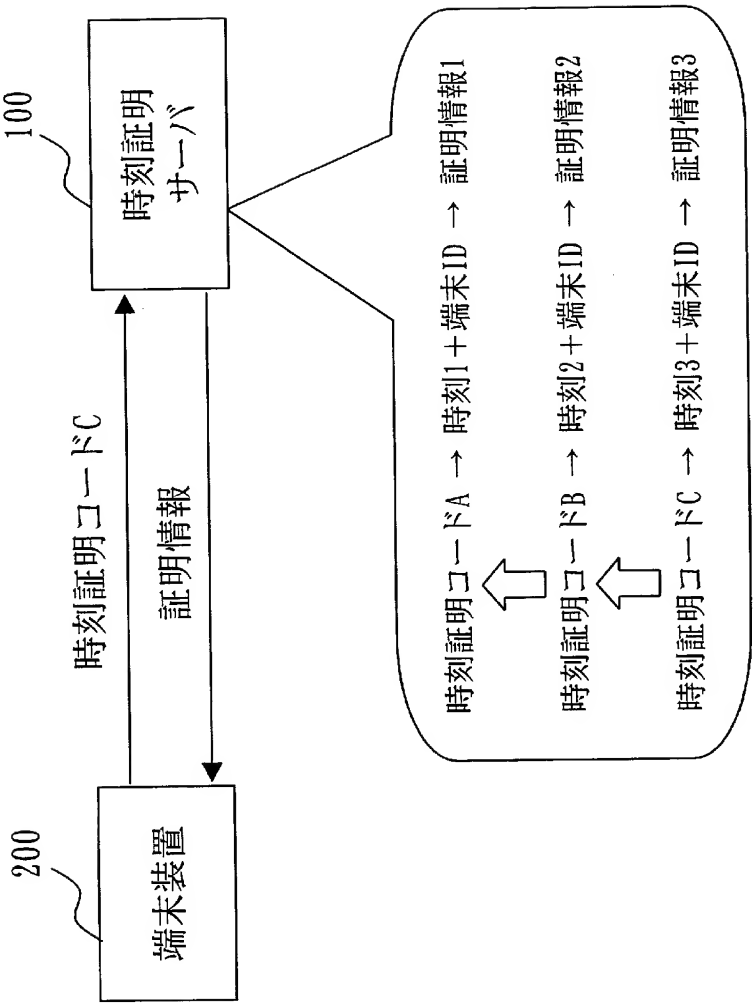

100
時刻証明
サーバ
時刻証明コードC
証明情報
200
端末装置
時刻証明コードA → 時刻1＋端末ID → 証明情報1
時刻証明コードB → 時刻2＋端末ID → 証明情報2
時刻証明コードC → 時刻3＋端末ID → 証明情報3

図 17

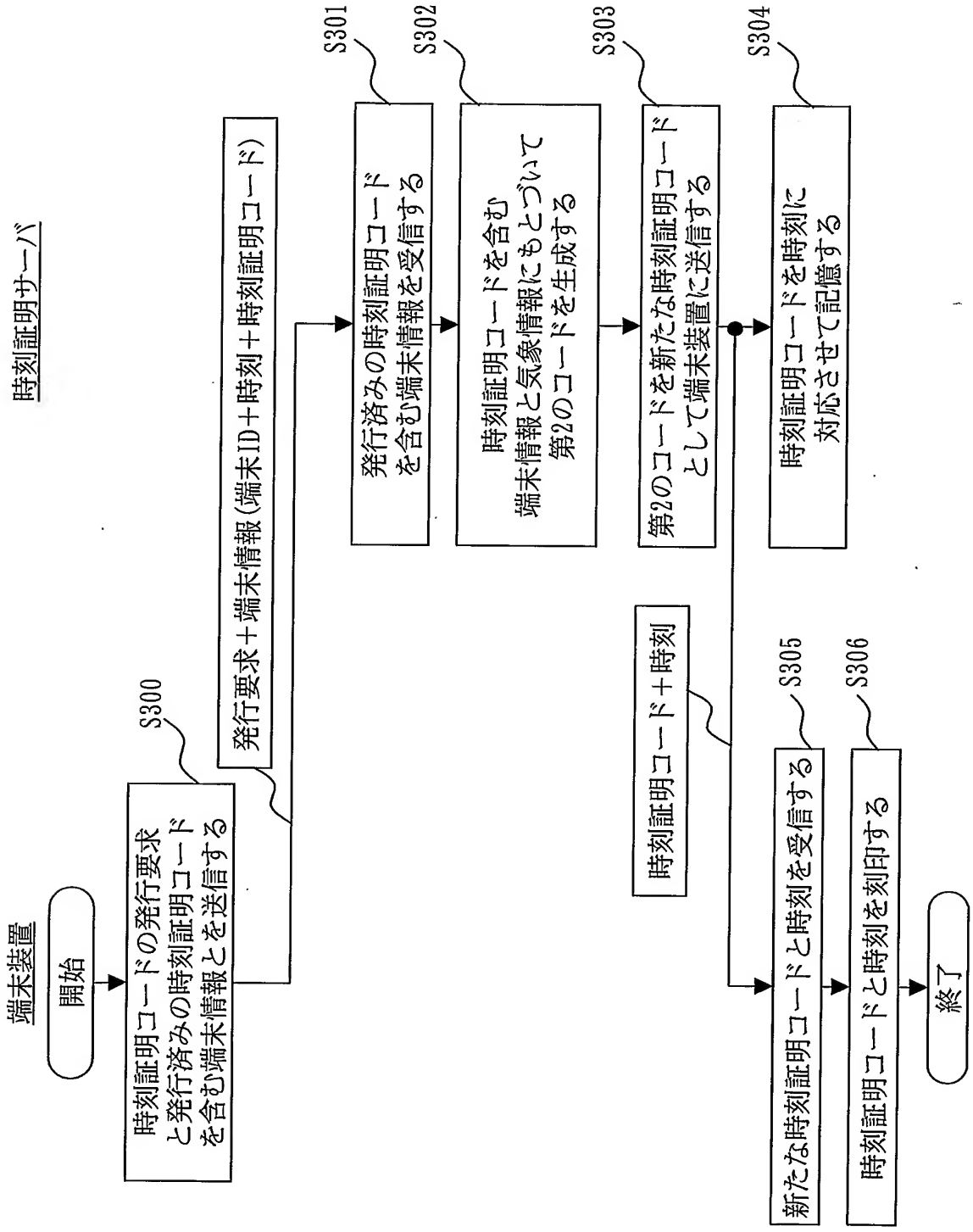
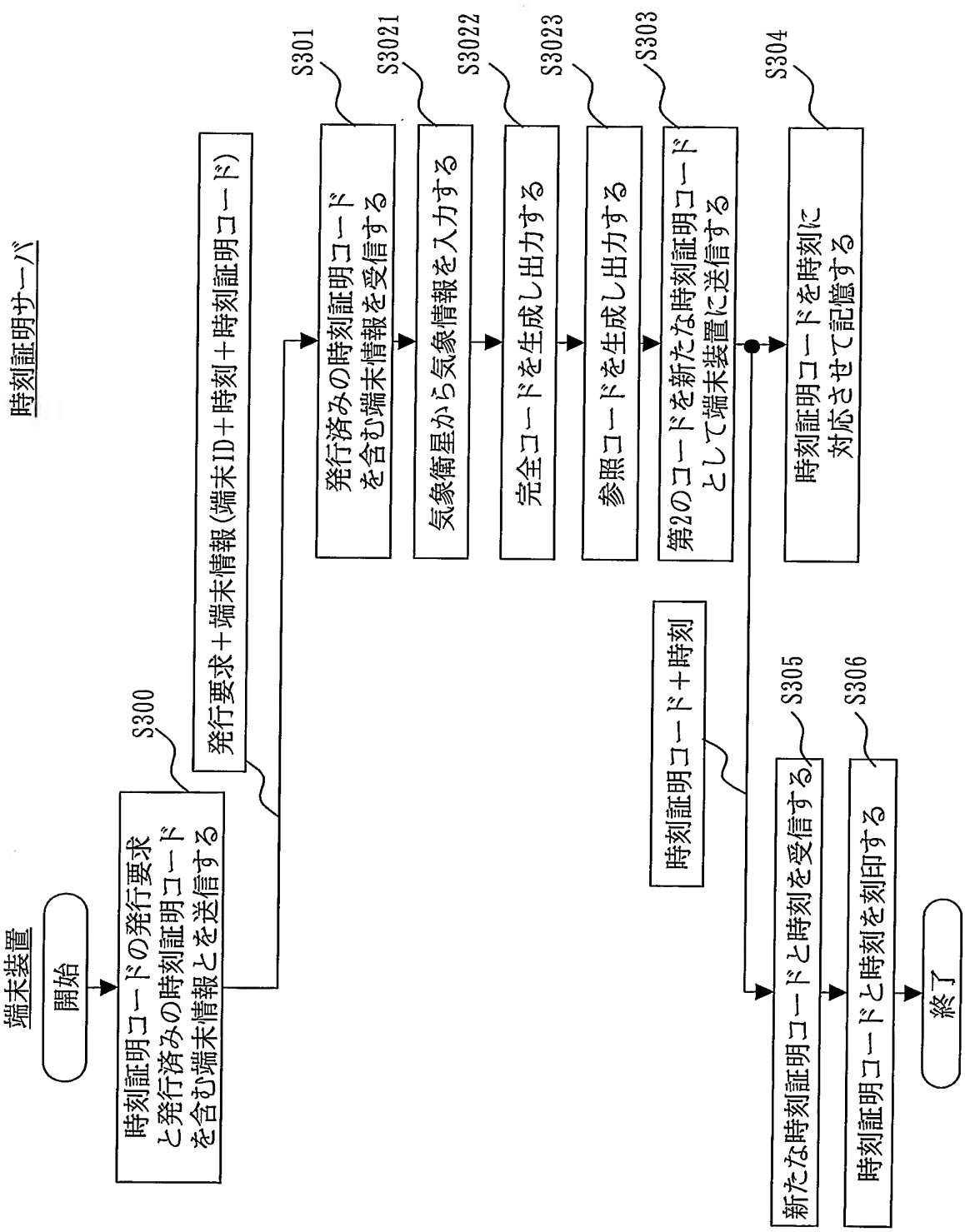

端末装置
時刻証明サーバ
開始
時刻証明コードの発行要求と発行済みの時刻証明コードを含む端末情報とを送信する
S300
発行要求＋端末情報(端末ID＋時刻＋時刻証明コード)
S301
発行済みの時刻証明コードを含む端末情報を受信する
S302
時刻証明コードを含む端末情報と気象情報にもとづいて第2のコードを生成する
S303
第2のコードを新たな時刻証明コードとして端末装置に送信する
S304
時刻証明コードを時刻に対応させて記憶する
時刻証明コード＋時刻
S305
新たな時刻証明コードと時刻を受信する
S306
時刻証明コードと時刻を刻印する
終了

図 18


端末装置
時刻証明サーバ
開始
時刻証明コードの発行要求と発行済みの時刻証明コードを含む端末情報とを送信する
S300
発行要求＋端末情報(端末ID＋時刻＋時刻証明コード)
S301
発行済みの時刻証明コードを含む端末情報を受信する
S3021
気象衛星から気象情報を入力する
S3022
完全コードを生成し出力する
S3023
参照コードを生成し出力する
S303
第2のコードを新たな時刻証明コードとして端末装置に送信する
S304
時刻証明コードを時刻に対応させて記憶する
時刻証明コード＋時刻
新たな時刻証明コードと時刻を受信する
S305
時刻証明コードと時刻を刻印する
S306
終了

[図19]

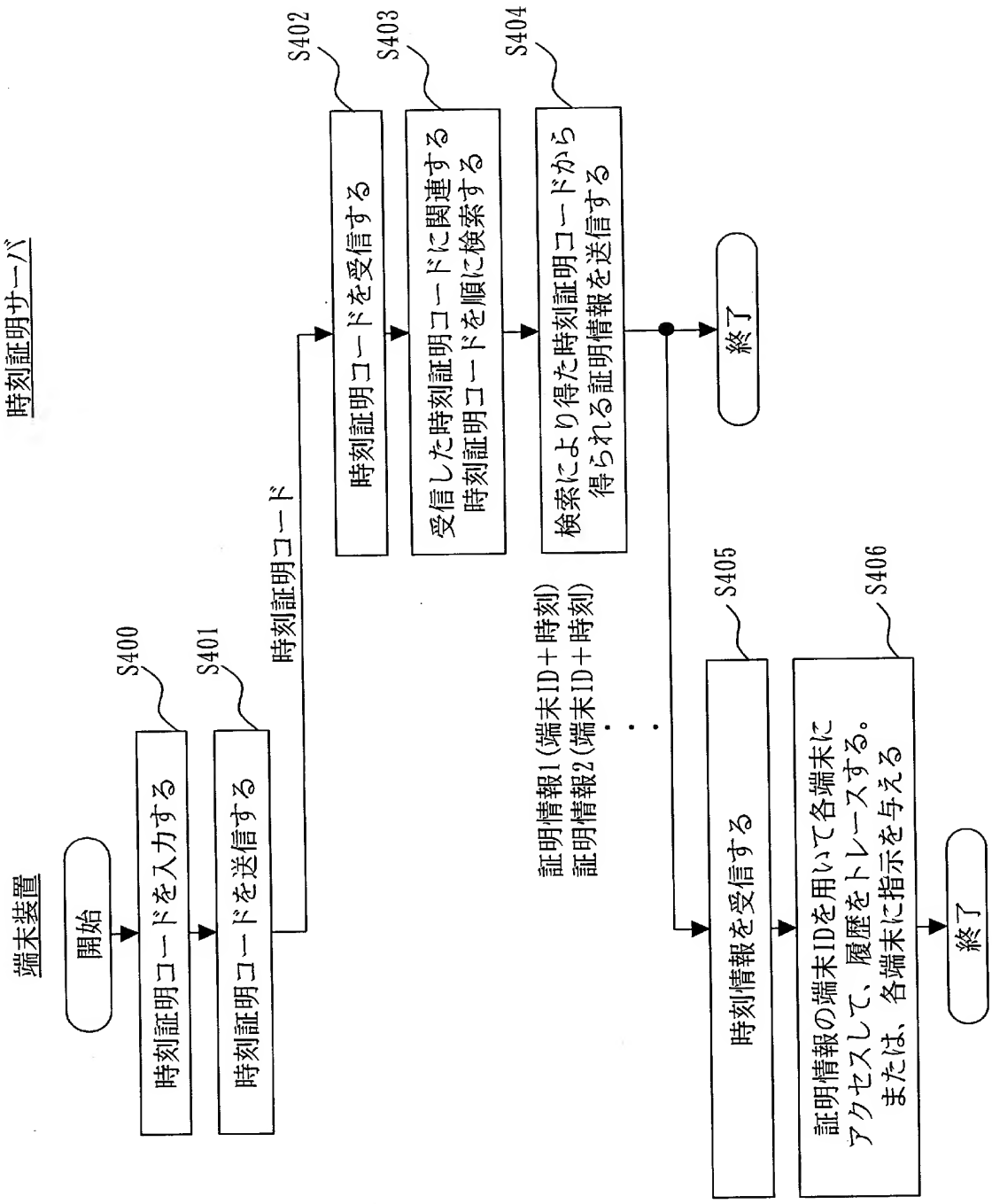

端末装置
時刻証明サーバ
開始
S400
時刻証明コードを入力する
S401
時刻証明コードを送信する
時刻証明コード
S402
時刻証明コードを受信する
S403
受信した時刻証明コードに関連する
時刻証明コードを順に検索する
S404
検索により得た時刻証明コードから
得られる証明情報を送信する
証明情報1(端末ID＋時刻)
証明情報2(端末ID＋時刻)
・
・
・
終了
S405
時刻情報を受信する
S406
証明情報の端末IDを用いて各端末に
アクセスして、履歴をトレースする。
または、各端末に指示を与える
終了

図 20

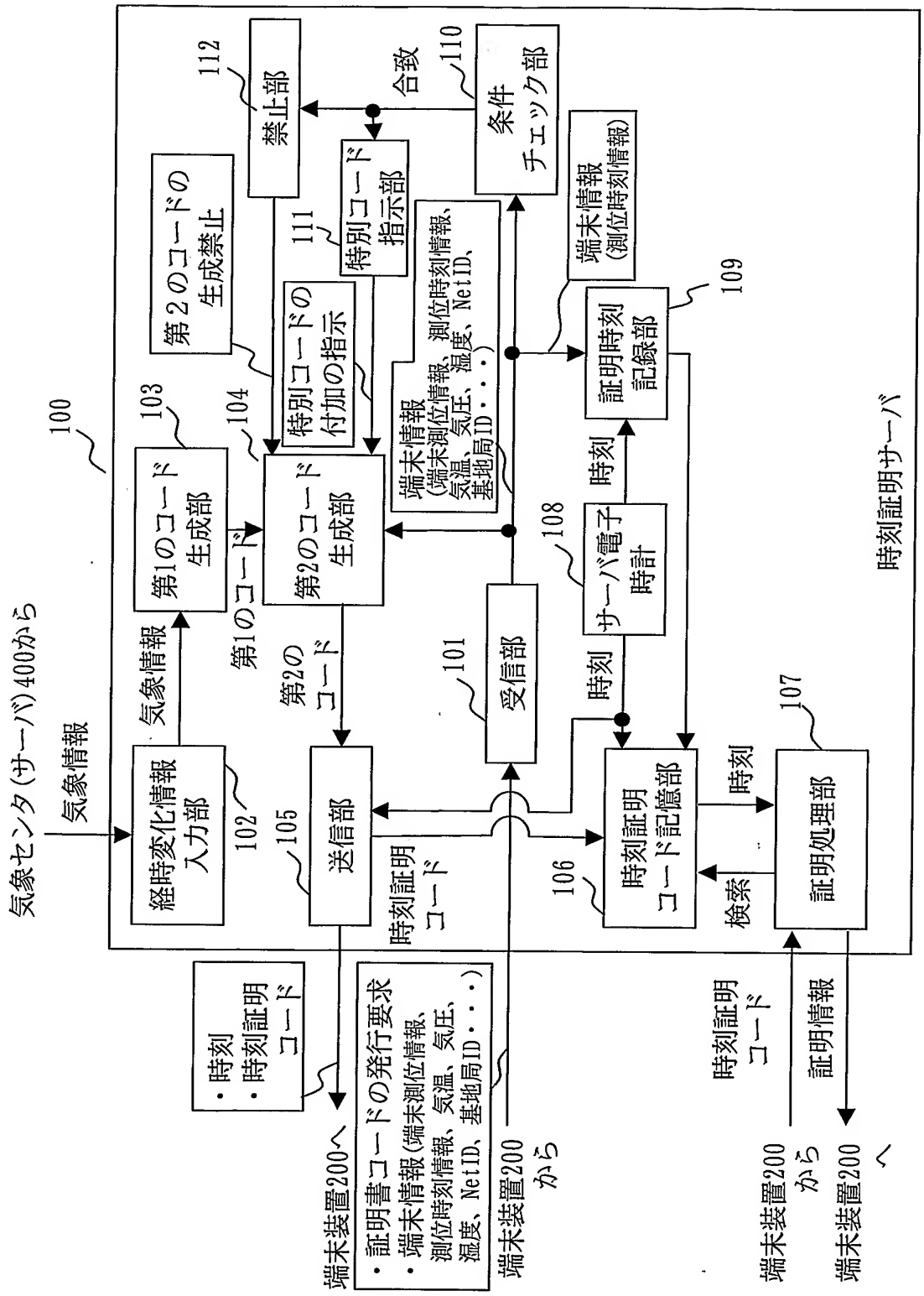

気象センタ(サーバ)400から
気象情報
100
経時変化情報入力部
102
気象情報
第1のコード生成部
103
第1のコード
第2のコード生成部
104
第2のコード
送信部
105
時刻証明コード
受信部
101
第2のコードの生成禁止
特別コードの付加の指示
禁止部
112
特別コード指示部
111
合致
条件チェック部
110
端末情報(端末測位情報、測位時刻情報、気温、気圧、温度、NetID、基地局ID・・・)
端末情報(測位時刻情報)
証明時刻記録部
109
時刻
サーバ電子時計
108
時刻
時刻証明コード記憶部
106
検索
時刻
証明処理部
107
時刻証明サーバ
・時刻
・時刻証明コード
端末装置200へ
・証明書コードの発行要求
・端末情報(端末測位情報、測位時刻情報、気温、気圧、温度、NetID、基地局ID・・・)
端末装置200から
時刻証明コード
端末装置200から
証明情報
端末装置200へ

図 21

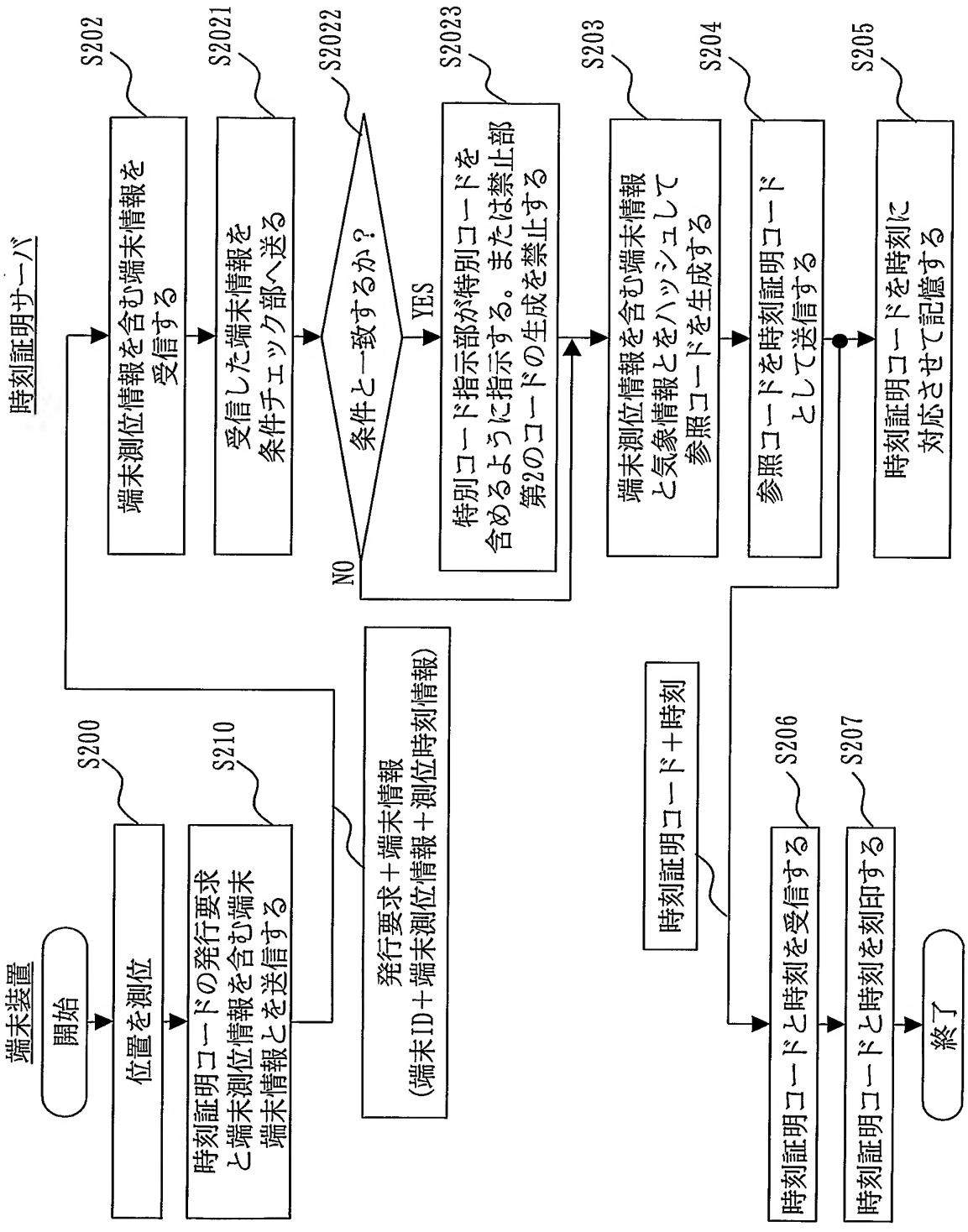
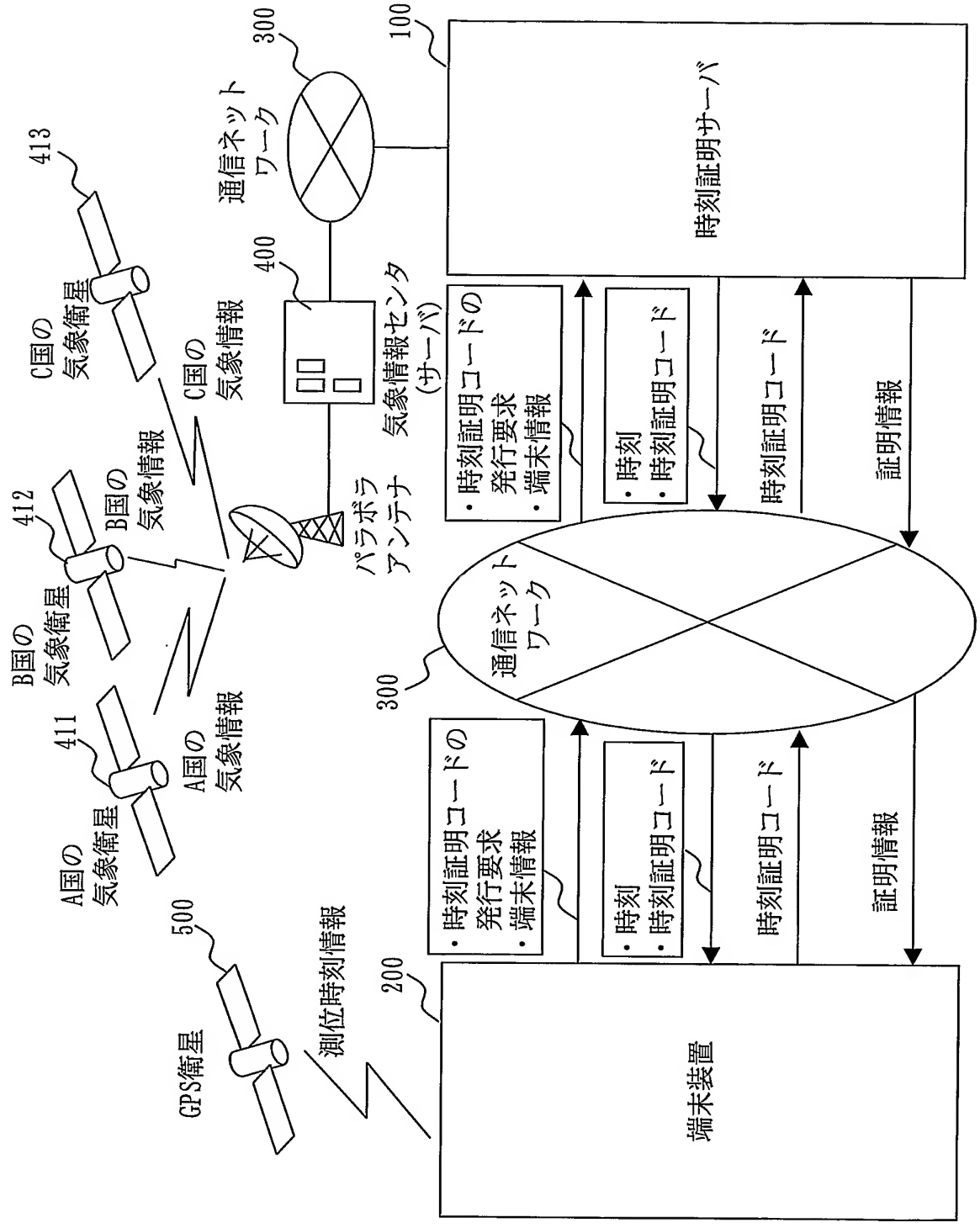

端末装置
開始
S200
位置を測位
S210
時刻証明コードの発行要求
と端末測位情報を含む端末
端末情報とを送信する
発行要求＋端末情報
(端末ID＋端末測位情報＋測位時刻情報)
時刻証明サーバ
S202
端末測位情報を含む端末情報を
受信する
S2021
受信した端末情報を
条件チェック部へ送る
S2022
条件と一致するか？
YES
NO
S2023
特別コード指示部が特別コードを
含めるように指示する。または禁止部
第2のコードの生成を禁止する
S203
端末測位情報を含む端末情報
と気象情報とをハッシュして
参照コードを生成する
S204
参照コードを時刻証明コード
として送信する
S205
時刻証明コードを時刻に
対応させて記憶する
時刻証明コード＋時刻
S206
時刻証明コードと時刻を受信する
S207
時刻証明コードと時刻を刻印する
終了

図 22


413
C国の
気象衛星
412
B国の
気象衛星
411
A国の
気象衛星
500
GPS衛星
C国の
気象情報
B国の
気象情報
A国の
気象情報
測位時刻情報
300
通信ネット
ワーク
400
パラボラ
アンテナ
気象情報センタ
(サーバ)
100
時刻証明サーバ
・時刻証明コードの
発行要求
・端末情報
・時刻
・時刻証明コード
時刻証明コード
証明情報
300
通信ネット
ワーク
・時刻証明コードの
発行要求
・端末情報
・時刻
・時刻証明コード
時刻証明コード
証明情報
200
端末装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/015896

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2001-297062 A (Mitsubishi Electric Corp.), 26 October, 2001 (26.10.01), (Family: none)	13,14 1-12,15-20
X A	JP 2002-215825 A (Mitsubishi Electric Corp.), 02 August, 2002 (02.08.02), (Family: none)	13,14 1-12,15-20
A	JP 2003-198539 A (Seiko Instruments Inc.), 11 July, 2003 (11.07.03), (Family: none)	1-20
A	Kazuya MIYAZAKI, "Denshi Bunsho ni Okeru Shomei to Time Stamp", Mitsubishi Denki Giho, 25 February, 2001 (25.02.01), Vol.75, No.2, pages 38 to 40	1-20

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 14 December, 2004 (14.12.04)	Date of mailing of the international search report 28 December, 2004 (28.12.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/015896

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Kazuya MIYAZAKI, "Secure Storage - Denshi Carteno Tekiyo -", Mitsubishi Denki Giho, 25 April, 2002 (25.04.02), Vol 76, No.4, pages 47 to 50	1-20

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１５８９６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ１７／６０

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ１７／６０，Ｈ０４Ｌ９／３２

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００４年
日本国登録実用新案公報	１９９４－２００４年
日本国実用新案登録公報	１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ，ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ２００１－２９７０６２Ａ（三菱電機株式会社） ２００１．１０．２６（ファミリーなし）	13, 14
Ａ		1-12, 15-20
Ｘ	ＪＰ２００２－２１５８２５Ａ（三菱電機株式会社） ２００２．０８．０２（ファミリーなし）	13, 14
Ａ		1-12, 15-20
Ａ	ＪＰ２００３－１９８５３９Ａ（セイコーインスツルメンツ株式会社） ２００３．０７．１１（ファミリーなし）	1-20

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １４．１２．２００４	国際調査報告の発送日　28.12.2004
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｌ　９１９４ 吉　田　耕　一 電話番号　０３－３５８１－１１０１　内線　３５６０

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	宮崎一哉，電子文書における署名とタイムスタンプ， 三菱電機技報，２００１．０２．２５，Vol.75，No.2，pp.38-40	1-20
Ａ	宮崎一哉 他，セキュアストレージ－電子カルテへの適用－， 三菱電機技報，２００２．０４．２５，Vol.76，No.4，pp.47-50	1-20